美国关键基础设施
安全防护体系与策略

孙利民　吕世超　李红　文辉　编著



清华大学出版社

美国关键基础设施安全防护体系与策略

孙利民　吕世超　李 红　文 辉　编著

清 华 大 学 出 版 社
北 京

内 容 简 介

关键基础设施作为国家经济、社会运行的神经中枢，一旦遭到物理或网络攻击，将会严重危害国家安全和国计民生。因此，许多国家都已经将关键基础设施安全作为一个国家安全战略问题来对待。本书介绍了美国在关键基础设施安全防护领域的布局，归纳了相关研究项目的技术报告，提炼出了关键技术，总结了先进经验。这些技术和经验，对于我国开展关键基础设施安全防护工作具有重要参考价值。

本书可供高等院校信息安全相关专业的学生、教师，各级政府部门的决策者及企业技术主管等阅读参考。

图书在版编目(CIP)数据

美国关键基础设施安全防护体系与策略/孙利民等编著. —北京：清华大学出版社，2017
ISBN 978-7-302-48639-8

Ⅰ. ①美…　Ⅱ. ①孙…　Ⅲ. ①基础设施－安全防护－研究－美国　Ⅳ. ①F299.712

中国版本图书馆 CIP 数据核字(2017)第 261701 号

责任编辑：薛　慧
封面设计：何凤霞
责任校对：赵丽敏
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：三河市铭诚印务有限公司
经　　销：全国新华书店
开　　本：170mm×230mm　　**印　　张**：18.75　　**字　　数**：346千字
版　　次：2017 年 12 月第 1 版　　**印　　次**：2017 年 12 月第1 次印刷
定　　价：98.00 元

产品编号：074100-01

前　言

关键基础设施作为国家经济、社会运行的神经中枢，包括公共通信和信息服务、能源、交通、金融、关键制造、食品和农业、政府设施和服务、公共卫生等重要行业和领域的信息和物理设施。这些关键基础设施设备或系统一旦遭到物理或网络攻击，将会严重危害国家安全和国计民生。因此，许多国家都已经将关键基础设施安全作为国家安全战略问题。

随着近年来工业化和信息化的不断融合，越来越多的基础设施系统不再封闭，逐渐开放接入到公共网络中，这将给关键基础设施系统带来越发严峻的网络安全威胁。近年来发生的诸如 Stuxnet、Duqu、Flame、Havex、BlackEnergy 和乌克兰大规模断电等重大安全事件证明了关键基础设施容易受到网络攻击的严重危害，在一定程度上促进了世界各国对关键基础设施安全防护的高度重视。

美国为了应对日益严峻的关键基础设施网络攻击安全威胁，历届政府通过发布一系列政策文件或部署关键技术研究项目等方式，推动该领域的理论研究与技术研发工作。作者在研究美国关键基础设施安全防护进展中，深入调研了美国国土安全部、能源部、国家标准与技术研究院、国家科学基金会和国防部先进研究项目局等部门的相关工作，从国家政策、研发项目、安全实践等方面总结归纳了这些部门近年来的科研工作。希望以此为我国在该领域的科学研究与项目部署提供一些参考意见。由于国家体制、文化及体系结构上的差异，我们需要辩证地来分析美国在关键基础设施安全方面所做的工作，有借鉴性地探索适合我国国情的发展战略和具体实施方法。

本书由中国科学院信息工程研究所物联网信息安全技术北京市重点实验室组织撰写，多位作者合作完成。其中，孙利民负责全书的组稿，并主持各个章节的撰写，负责全书的审校。第 1 章由孙利民执笔完成，第 2、4、6 章由吕世超执笔完成，第 3 章、附录 A 和附录 B.1 由李红执笔完成，第 5 章、附录 B.2 和附录 B.3 由文辉执笔完成。

由于时间仓促及水平有限，本书难免有错漏之处，希望读者不吝批评指正。如有机会，我们将在后续的版本中更新修改，也会结合今后的研究工作继续补充内容。若有任何意见，请发送至 lvshichao_iie@126.com。

本书涉及的研究课题得到科技部国家重点研发计划项目“脆弱性分析与威胁态势感知技术”（项目编号：2016YFB0800202）、北京市科学技术委员会项目“国家关键基础设施安全监管平台核心技术研究”（项目编号：Z161100002616032）、国家自然科学基金项目“网络空间中工控设备快速发现与精细识别关键技术研究”（项目编号：U1536107）、国家自然科学基金项目“针对电网工控系统的协同入侵检测技术研究”（项目编号：61702506）等资助。

本书在撰写过程中得到了中国科学院信息工程研究所孟丹所长、孙德刚副所长等领导的指导和帮助，在此一并向他们表示衷心的感谢。

作者

2017 年 7 月于北京

目　　录

图 目 录

表 目 录

第1章　关键基础设施安全概述

1.1　关键基础设施含义

关键基础设施是指公共通信和信息服务、能源、交通、水利、金融、化学、关键制造、食品和农业、政府设施和服务、公共卫生、国防军工、电子政务等重要行业和领域的重要信息和物理设施。作为经济、社会运行的神经中枢，这些设施一旦遭受来自物理和网络空间的破坏、丧失功能或者数据泄露，就可能严重危害国计民生、公共利益和国家安全。

1.1.1　中国政府高度重视关键信息基础设施安全

党的十八届三中全会通过了《关于全面深化改革若干重大问题的决定》(简称《决定》)[1]。《决定》明确指出，“加大依法管理网络力度，加快完善互联网管理领导体制，确保国家网络和信息安全。设立国家安全委员会，完善国家安全体制和国家安全战略，确保国家安全。”为了贯彻落实十八届三中全会精神，健全公共安全体系，领导中国从网络大国迈向网络强国，中央网络安全和信息化领导小组于2014年2月27日宣告成立。中共中央总书记、国家主席、中央军委主席习近平担任组长，国务院总理李克强和中央书记处书记刘云山担任副组长。自中央网络安全和信息化领导小组成立以来，中国领导人高度重视关键信息基础设施网络安全问题，在小组全体会议、座谈会等重要场合发表了一系列重要讲话，分析了如何正确处理网络安全和发展的关系，阐述了网络强国战略及其实施举措。

1. 中央网络安全和信息化领导小组第一次会议[2]

习近平总书记在2014年2月27日，主持召开了中央网络安全和信息化领导小组第一次全体会议，并发表了重要讲话。讲话指出：“没有网络安全就没有国家安全，没有信息化就没有现代化。建设网络强国，要有自己的技术，有过硬的技术；要有丰富全面的信息服务，繁荣发展的网络文化；要有良好的信息基础设施，形成实力雄厚的信息经济。”习总书记本次讲话提到的信息基础设施，主要

指在政治、经济、文化、社会、军事等领域用于信息采集、处理、传播和利用的信息系统和网络。

2. 习近平总书记4·19讲话[3]

习总书记在2016年4月19日网络安全和信息化座谈会上讲话指出,“加快构建关键信息基础设施安全保障体系。金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢,是网络安全的重中之重,也是可能遭到重点攻击的目标。‘物理隔离’防线可被跨网入侵,电力调配指令可被恶意篡改,金融交易信息可被窃取,这些都是重大风险隐患。不出问题则已,一出就可能导致交通中断、金融紊乱、电力瘫痪等问题,具有很大的破坏性和杀伤力。我们必须深入研究,采取有效措施,切实做好国家关键信息基础设施安全防护。”

3. 习近平主持召开国家安全工作座谈会[4]

习总书记在2017年2月17日召开的国家安全座谈会上强调,“要准确把握国家安全形势,牢固树立和认真贯彻总体国家安全观,以人民安全为宗旨,走中国特色国家安全道路,努力开创国家安全工作新局面,为中华民族伟大复兴中国梦提供坚实安全保障。”在部署对当前和今后一个时期国家安全工作时,明确提出,“要筑牢网络安全防线,提高网络安全保障水平,强化关键信息基础设施防护,加大核心技术研发力度和市场化引导,加强网络安全预警监测,确保大数据安全,实现全天候全方位感知和有效防护。”习总书记将关键信息基础设施安全问题作为国家安全问题来看待。由此可见,国家领导人高度重视关键信息基础设施安全。

4. 2016年3月政府工作报告[5]

李克强总理2016年3月5日在第十二届全国人民代表大会第四次会议上做的政府工作报告中多次提到了基础设施建设工作。在“十三五”时期主要目标任务和重大举措的推进新型城镇化和农业现代化,促进城乡区域协调发展方面指出:“加强重大基础设施建设,高铁营业里程达到3万公里、覆盖80%以上的大城市,新建改建高速公路通车里程约3万公里,实现城乡宽带网络全覆盖。”在2016年重点工作中的改善农村公共服务方面指出:“加大农村基础设施建设力度,新建改建农村公路20万公里,具备条件的乡镇和建制村要加快通硬化路、通客车。抓紧新一轮农村电网改造升级,两年内实现农村稳定可靠供电服务和平原地区机井通电全覆盖。实施饮水安全巩固提升工程。推动电子商务进农村。

建设美丽宜居乡村”。在安全生产和公共安全方面指出:“加强安全基础设施和防灾减灾能力建设,健全监测预警应急机制,提高气象服务水平,做好地震、测绘、地质等工作。完善和落实安全生产责任、管理制度和考核机制,实行党政同责、一岗双责、失职追责,严格监管执法,坚决遏制重特大安全事故发生,切实保障人民生命财产安全。”

分析政府工作报告中与基础设施相关的内容可知,基础设施的范围比信息基础设施要大,基础设施不仅包括用来保障金融、能源、电力、交通等领域系统正常运作的电信和广播电视等网络空间的系统和网络,还包括为人民生产生活提供公共服务的工程设施,如公路、铁路、电网、水利等物理空间设施。即基础设施既包括网络空间的信息基础设施,也包括物理空间的工程设施。

5. “一带一路”推进能源基础设施互联互通[6]

李克强总理在 2016 年 11 月 17 日主持召开的国家能源委员会会议上指出,“能源战略是国家发展战略的重要支柱,保障国家能源安全需要统筹国内国际两个大局,既要立足国内,又要深化国际合作,形成多元稳定的供给格局。要巩固与传统资源国家的互利合作,优化能源贸易结构,抓住‘一带一路’建设重大机遇,推进能源基础设施互联互通,加大国际产能合作,带动有竞争优势的能源装备出口。积极参与全球能源治理,推动国际能源秩序和治理体系朝着更加公正合理的方向发展。”

能源指煤炭、石油、天然气、生物质能和电力、热力以及其他直接或者通过加工、转换而取得有用能的各种资源[7]。作为基础设施的一个重要领域,能源是国民经济发展的重要物质基础。中国政府高度重视能源基础设施互联互通建设工作。

1.1.2　中国政府相关文件

1. 国务院

国务院办公厅于 2007 年 9 月 18 日发布了《关于开展重大基础设施安全隐患排查工作的通知》(国办发〔2007〕58 号)[8],通知要求,重点做好“公路交通设施、铁路交通设施、水运交通设施、民航交通设施、大型水利设施、大型煤矿、重要电力设施、石油天然气设施、城市基础设施”九个对象的安全隐患排查工作。国务院办公厅指出的上述九类基础设施都属于重大、关键基础设施范畴,都是指那些关乎国计民生的核心基础设施。

国务院办公厅于2012年6月28日发布了文件《关于大力推进信息化发展和切实保障信息安全的若干意见》(国发〔2012〕23号)[9]。该文件在健全安全防护和管理,保障重点领域信息安全的保障工业控制系统安全方面指出:“加强核设施、航空航天、先进制造、石油石化、油气管网、电力系统、交通运输、水利枢纽、城市设施等重要领域工业控制系统,以及物联网应用、数字城市建设中的安全防护和管理,定期开展安全检查和风险评估。重点对可能危及生命和公共财产安全的工业控制系统加强监管。对重点领域使用的关键产品开展安全测评,实行安全风险和漏洞通报制度。”工业控制系统广泛应用于上述领域的基础设施中,实现设施和系统的自动化控制和运行操作,是基础设施的核心组成部分。这些基础设施的安全防护重点就是保障工业控制系统的网络和物理安全。

国务院于2013年9月6日发布了文件《关于加强城市基础设施建设的意见》(国发〔2013〕36号)[10]。文件指出,城市基础设施是城市正常运行和健康发展的物质基础,并建议,“加强城市道路交通基础设施建设,加大城市管网建设和改造力度,加快污水和垃圾处理设施建设,加强生态园林建设。”城市基础设施是国家关键基础设施的缩影和典型代表,城市中的道路、水/电/天然气管网、污水和垃圾处理系统等组成了城市的骨架,这些基础设施的完善程度影响着城市的承载能力及人民的生活质量。

2. 工业和信息化部

工信部于2014年8月29日发布了《关于加强电信和互联网行业网络安全工作的指导意见》(工信部保〔2014〕368号)[11],在加强新技术新业务网络安全管理重点工作中指出:“加强对云计算、大数据、物联网、移动互联网、下一代互联网等新技术新业务网络安全问题的跟踪研究,对涉及提供公共电信和互联网服务的基础设施和业务系统要纳入通信网络安全防护管理体系,加快推进相关网络安全防护标准研制,完善和落实相应的网络安全防护措施。”提供公共电信和互联网服务的网络和系统都属于信息基础设施的范畴。

工信部于2011年10月27日发布了《关于加强工业控制系统信息安全管理的通知》(工信部协〔2011〕451号)[12]。通知指出:“数据采集与监控(SCADA)、分布式控制系统(DCS)、过程控制系统(PCS)、可编程逻辑控制器(PLC)等工业控制系统广泛运用于工业、能源、交通、水利以及市政等领域,用于控制生产设备的运行。一旦工业控制系统信息安全出现漏洞,将对工业生产运行和国家经济安全造成重大隐患。加强工业控制系统信息安全管理的重点领域包括核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、

城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关的领域。”上述关键基础设施都是指事关国家、经济发展命脉的重要工业控制设备、网络和系统。

3. 网络安全法

2016 年 11 月 7 日，第十二届全国人民代表大会常务委员会第二十四次会议通过了《中华人民共和国网络安全法》(简称《网络安全法》)[13]。该法案专门设立了一节对关键信息基础设施的运行安全做出了具体的法律规定，对关键信息基础设施运行安全不仅给出了定义，规定了如何实施安全保护，而且还从国家相关部门、行业、关键基础设施/网络运营者等不同层面分别规定了国家网信部门、行业主管单位、运营单位或企业等各自的义务与责任。

其中，《网络安全法》的第三章网络运行安全的第二节关键信息基础设施的运行安全的第三十一条规定：“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。”与其他定义相比，《网络安全法》对关键信息基础设施的定义又新增加了网络安全等级保护和重点保护的要求。

4. 国家互联网信息办公室

经中央网络安全和信息化领导小组批准，国家互联网信息办公室于 2016 年 12 月 27 日发布了《国家网络空间安全战略》(简称《战略》)[14]，将保护关键信息基础设施作为一项重点战略任务。《战略》指出：“国家关键信息基础设施是指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。采取一切必要措施保护关键信息基础设施及其重要数据不受攻击破坏。坚持技术和管理并重、保护和震慑并举，着眼识别、防护、检测、预警、响应、处置等环节，建立实施关键信息基础设施保护制度，从管理、技术、人才、资金等方面加大投入，依法综合施策，切实加强关键信息基础设施安全防护。”《战略》不仅给出了关键信息基础设施较为全面的定义，还重点强调了信息基础设施和其关键数据的同等重要性。

经中央网络安全和信息化领导小组批准，2016 年 7 月 8 日，首次全国范围的关键信息基础设施网络安全检查工作启动[15]。检查时间截至 2016 年 12 月底。本次检查给出了关键信息基础设施的如下定义："关键信息基础设施指的是面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，这些系统一旦发生网络安全事故，可能影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境及人民生命财产造成严重损失。"本次安全检查给出的关键信息基础设施定义，将关键信息基础设施定义为提供网络信息服务或支撑重要行业运行的信息系统或工业控制系统。该定义突出强调了信息系统和工业控制系统在关键信息基础设施中的同等重要性。

国家互联网信息办公室于 2017 年 7 月 11 日发布了《关键信息基础设施安全保护条例（征求意见稿）》[16]。该条例是依据《网络安全法》，专门针对关键信息基础设施安全制定的条例。在该条例的第三章第十八条给出了关键信息基础设施保护范围："下列单位运行、管理的网络设施和信息系统，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的，应当纳入关键信息基础设施保护范围：（一）政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位；（二）电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位；（三）国防科工、大型装备、化工、食品药品等行业领域科研生产单位；（四）广播电台、电视台、通讯社等新闻单位；（五）其他重点单位。"此外，该条例也在关键信息基础设施运营者安全保护、产品和服务安全、监测预警、应急处置和检测评估等方面给出了具体要求及法律责任规定。

1.1.3 美国政府关键基础设施安全布局

随着关键基础设施行业中越来越多的系统网络接入公共网络，基础设施系统面临着越发严峻的网络安全问题。美国也已经将关键基础设施安全提升为国家战略问题。美国自克林顿政府就开始重视关键基础设施安全问题。克林顿、小布什、奥巴马和特朗普政府在国家安全战略、机构设置、安全保护计划及项目、标准规范等方面持续开展并推动了关键基础设施安全保护工作布局，通过一系列政策文件从法律、政府层面引导、促进关键基础设施安全建设工作。关于这些具体政策文件的介绍请参见 1.4 节内容。

1996 年 7 月 15 日，在克林顿政府颁布的第 13010 号行政令《关键基础设施防护》[17]中指出，关键基础设施包括电信、电力、天然气石油存储和运输、银行和

金融、交通、水利供应、应急服务（如医疗、警务、火警和救援）及其他保障政府持续运作 8 类系统。由于许多关键基础设施都是由私营企业拥有和经营的，因此，13010 号行政令还宣布成立总统关键基础设施保护委员会，要求政府部门与相关私营企业一起合作来研发、部署安全防护技术。

1998 年 5 月 22 日，克林顿总统颁布了第 63 号总统决策指令《关键基础设施防护》[18]。该指令在明确关键基础设施定义和范畴的基础上，进一步明确了财政部、司法部、国防部、商业部、交通部、能源部等相关部门的责任与义务。

小布什总统上任后不久便发生了“9·11”恐怖袭击事件，因此，为了应对恐怖袭击活动，加强基础设施安全防护措施，2001 年 10 月 16 日，小布什政府颁布了第 13231 号行政令《信息时代的关键基础设施防护》[19]。该行政令指出，信息时代的商业交易、政府运作和国家防御都依赖的关键信息基础设施涉及电信、能源、金融服务、制造业、水利、交通、医疗保健和应急服务等行业和领域。第 13231 号行政令还宣布成立总统关键基础设施保护管理委员会，并要求委员会关于关键基础设施保护工作、安全项目建设等方面定期提出发展建议和政策。

为了进一步组织开展具体安全防护项目，2002 年 11 月 25 日，小布什总统签署了《国土安全法案》[20]，宣布成立国土安全部，专门负责国土安全事务，具体包括防止发生针对关键基础设施的恐怖袭击事件，加强安全防范能力，保卫网络空间安全，增强自然灾害应对能力等。国土安全部自成立以来针对关键基础设施网络安全，设计了专门的机构，开展了一系列安全实践和研发项目，如设计了工业控制系统网络应急响应小组，开展了“网络风暴”系列演习，发起了“国家基础设施保护计划”和“下一代网络基础设施”项目等。

为了动员和组织全国上下共同抵御恐怖袭击活动，小布什政府于 2002 年 7 月 16 日发布了《国土安全国家战略》第一版[21]。随后，在 2003 年 2 月，小布什总统发布了《关键基础设施和重要资产物理保护国家战略》[22]，将农业和食品、水利、公共健康、应急服务、国防工业基础、电信、能源、交通、银行和金融、化学工业和危险材料、邮政和航运等设施作为关键基础设施，将国家古迹和建筑、核电站、大坝、政府设施、商业设施作为重要资产。2006 年，国土安全部发起了《国家基础设施保护计划》[23]。该计划的目标是通过加强对国家关键基础设施和重要资产的保护，来建立一个物理上、信息网络上更安全以及故障恢复能力更强的美国，以此来阻止、减缓或消除由恐怖袭击所带来的蓄意破坏影响。

奥巴马总统上任后，继续加强了关键基础设施安全防护力度。2013 年 2 月 12 日，奥巴马政府同时颁布了第 13636 号行政令《提高关键基础设施的网络安全》[24]和第 21 号总统决策指令《提高关键基础设施的安全性和恢复力》[25]。前

者旨在指导行政部门设计一个技术中立的网络安全框架。后者则明确定义了16个关键基础设施行业,包括化学、商业设施、通信、关键制造、大坝、国防军工、应急服务、能源、金融服务、食品和农业、政府设施、公共卫生、信息技术、核反应堆材料和废物、交通、城市供水和废水处理系统。

在第13636号行政令和第21号总统决策指令的指导要求下,美国国家标准与技术研究院起草,美国白宫于2014年2月12号公布了《提高关键基础设施网络安全的框架规范》(简称《规范》)[26]的第一个版本。该规范是自美国启动保护关键基础设施信息安全工作以来发布的第一个较全面的基础性指导文件。为了进一步加强网络安全法律、法规保护力度,奥巴马总统于2015年12月18日签署了《网络安全信息共享法案(2015)》[27],并将其标注为《2015年网络安全法案》。该法案第208条专门对"多重并发的关键基础设施网络事件"给出了法律规范。除了通过立法来促进改善国家网络安全以外,奥巴马政府还在2016年2月9日推行了《网络安全国家行动计划》[28],在提升国家整体网络安全水平方面,该行动计划明确指出,要增强关键基础设施的安全性和恢复力。

特朗普总统上任后开始全面加强网络安全建设。特朗普总统于2017年5月11日签署了网络安全行政令《增强联邦网路和关键基础设施的网络安全》[29],在联邦网络、关键基础设施和国家三个方面,规定了增强网络安全的措施。在关键基础设施网络安全方面,该项行政令要求应遵照奥巴马政府颁布的第21号总统决策指令所规定的关键基础设施行业进行安全评估,并于180日内提交其网络安全风险评估报告,今后每年度评估一次并更新报告。

小结:中国政府和美国政府都高度重视关键基础设施在网络空间所面临的安全威胁和攻击问题。二者分别通过领导人重要讲话、政府文件等形式在不同场合强调了开展关键基础设施安全防护工作的必要性,阐述了关键基础设施的含义和范畴,成立了专门的网络安全机构,发布了安全法律法规、国家安全战略及安全保护计划等重要文件。

1.2 典型安全事件

在现代战争时期,敌对双方首要摧毁目标必然是指挥机构,其次便是国家正常运行所依赖的电力、石油、天然气、交通以及水利等关键基础设施,从而实现以点破面,使整个国家陷入瘫痪的目的。目前较为突出的是在海湾战争和科索沃战争中,美军通过"斩首行动"迅速破坏了敌方的高级指挥机构和众多电力、能

源、通信、机场等关键基础设施，导致伊军和南联盟很快地失去了指挥权进而陷入一片混乱。

在目前总体和平的情况下，一些国家政府雇佣的高度组织化和专业化的黑客团体，以及一些以敲诈勒索为手段来营利的黑客团伙，这些组织和个人在近几年给各国的关键基础设施带来了不少的混乱和麻烦，也引起了业内业外的广泛关注。工业控制系统是关键基础设施的核心组成部分，因此，工控系统也就成了安全攻击的首要对象。目前发生在工控领域的安全事件得到了世界各国的广泛关注。下面就国内外发生在能源、水利、污水处理、交通以及制造业等领域的安全事件，分别叙述其起因、经过及影响。

1. 能源行业

（1）“震网”病毒

“震网”病毒于 2010 年 6 月席卷伊朗、印度尼西亚和印度，其中伊朗关键基础设施感染最为严重，尤其是核电站的浓缩铀设备的离心机遭到破坏，造成伊朗核电站推迟发电、重新更换设备、核泄漏等一系列重大安全后果。“震网”病毒可以自我复制，通过网络或 USB 等介质不断扩散。仅伊朗国内就有 500 万网民和多个行业的领军企业感染了“震网”病毒。

首先，“震网”病毒的入侵方式是精心设计的。这次事件的主要受害者 Natanz 工厂，负责着伊朗的核项目，拥有 15 层防火墙、3 个数据单向保护设备和入侵检测系统，这么强大的保护网之所以都未能阻止“震网”病毒的渗透攻击，是因为“震网”病毒采取了极为巧妙的攻击策略。“震网”病毒的编写人员在 2009 年创建之日起便定向攻击了和 Natanz 工厂相关联的几家电力设施、工业自动化系统及铀浓缩离心机供应商，设计者通过精心设计，悄无声息地渗透了这些企业网络，从中搜集和“Step 7”软件相关的信息，并利用在其中一家工控系统供应商为 Natanz 工厂系统升级改造的时机，通过移动介质将“震网”病毒引入了 Natanz 工厂系统中。

其次，“震网”病毒的设计也极为复杂。2010 年曝光于公众视野范围内的只是“震网”简单版本，然而，“震网”的复杂变种版本才是那个让伊朗政府极为不安的不定时炸弹。2007 年有人在 VirusTotal 上提交了段代码，这在后来被证实为“震网”的第一个变种，即复杂变种版本。大家所熟悉那个简单版本，其相较于复杂版本更为简单，也缺乏隐蔽性，只是能够控制离心机的转速使其周期性大幅改变，从而破坏离心机。但是，Natanz 工厂为了弥补离心机不稳定而配置的级联保护系统，能够防止离心机坏掉，防止发生生产流程终止情况。所以，“震网”病

毒简单版本并不是那个影响力最大的。复杂变种版本是最早入侵并潜伏在Natanz工厂工业控制系统中的,其主要目的并不是大肆破坏,而是通过伪装数字签名来表现为一个合法软件。在控制室、报警系统和操作员看来,系统运行状态一切正常。“震网”病毒复杂变种版本小心翼翼地控制着隔离阀,增大压力,慢慢减少转子的寿命,但不马上损坏离心机,从而增强了隐蔽性。

然而,“震网”病毒也不是完全隐蔽的。其开始是针对伊朗核设施设计的,但是在感染民用主机的同时,也将自身暴露于公众视野之下,许多安全公司都针对“震网”病毒的攻击模式和路径加固了安全防护措施。“震网”病毒无疑是网络空间的一枚核弹,其造成的影响和破坏不局限于伊朗,它刷新了人们对21世纪网络战争的认知,一个国家以较低的代价便可以在网络空间对另一方造成巨大的破坏。

(2)“火焰”蠕虫

2012年,美国和以色列为了破坏伊朗的核计划使用“火焰(Flame)”蠕虫进行了大量的恶意攻击。2012年5月,“火焰”蠕虫由于在以色列的策划下对伊朗的石油工业发起了一系列攻击,由此进入了公众视野。虽然,此次行动中,以色列成为了替罪羔羊,但“火焰”蠕虫据称是由美国和以色列共同研究设计而完成的,甚至有西方某官员称,策划者有NSA、CIA、以色列军队和Stuxnet的设计团队等,在如此强大的团队共同努力下,“火焰”蠕虫也就成为迄今为止最为复杂的恶意软件。即使是国家级的安全网络,仍然会感染“火焰”蠕虫。感染后果包括:用户的浏览器记录、键盘、账号密码、通话记录等敏感信息都会被回传到C&C服务器,摄像头和麦克风遭受非授权访问控制,地理位置信息数据遭受泄露等。下面从“火焰”的传播路径、复杂结构、隐蔽性三个特点描述这一蠕虫病毒。

“火焰”主要通过物理接触和远程感染两种方式在伊朗的关键基础设施领域扩散,安全研究人员在捕获的“火焰”样本中发现了“震网”病毒所使用的USB攻击模块。一些人会将感染了“火焰”蠕虫的USB插入到关键基础设施系统中的PC机中。另一种传播方式则是通过Windows Update,将冒用微软数字签名的“火焰”蠕虫从伪造的服务器下载安装到受害者电脑上,由此躲过杀毒软件的检测。

“火焰”蠕虫的复杂性体现在:拥有5种以上不同的加密算法,3种以上压缩技术,至少5种文件格式。“火焰”是用不太常见的LUA语言(一般用在游戏机上)编写的,其总体大小在30MB左右。“火焰”代码有大量的独立模块和攻击工具包,其中主模块文件大小在6MB之上,其他模块则有漏洞攻击代码、模块配置

文件、信息盗取模块等。“火焰”还会将窃取的系统信息以高度结构化的格式存储在 SQLite 等数据库中。

“火焰”的隐蔽性体现在：通过伪造终端服务产品的 CA 证书来伪装自己，进而不被杀毒软件轻易发现。“火焰”的行动策略异常狡猾，即在感染“火焰”的计算机具有反病毒保护程序时，“火焰”会停止可能引起安全应用程序进行主动检测行为的一些行动和恶意代码的执行。但是，尽管如此，微软也及时发布了“灭火”补丁并新增三个证书授权来缓解 Windows 用户遭受的威胁，各安全软件公司也分别推送了补丁和更新升级服务。

(3) “Havex”恶意软件

2014 年，欧美国家约有 1000 多家能源控制系统和机械设备公司被新型恶意软件“Havex”感染入侵。“Havex”主要被用来感染 SCADA 和工控系统中使用的工业控制软件。据媒体报道，“Havex”攻击性极强，有能力禁用水电大坝、使核电站过载以及一键式关闭国家电网。但实际上，“Havex”主要以窃取数据情报为目的，通过 OPC 层层入侵，一是获取能源工厂的过程控制系统的拓扑结构，进而可以实现对控制系统底层终端的控制；二是偷窃炼油、制药以及机械设备的配方或制作方案等。

虽然“Havex”恶意软件只包括一个通用的远程木马和用 PHP 编写的服务器程序，但是它的传播方式在当时极具创新性，除了传统的利用漏洞渗透工具包和垃圾邮件感染外，还采用了“水坑”式攻击方式，即通过渗透到目标软件公司的 Web 站点，在合法软件中加入恶意代码。随后一旦用户下载并安装被篡改的升级软件包，恶意软件就会自动安装并释放一个“mbcheck.dll”文件，这个恶意代码作为攻击者的后门渗透到工业控制系统网络中，C&C 服务器会指示被感染的计算机下载并执行其他组件。在此基础上，“Havex”的信息搜集组件会扫描本地网络中那些会对 OPC(开放平台通信标准)请求做出响应的设备，收集这些设备的操作系统信息，窃取存储在 Web 浏览器的密码，然后，使用自定义协议将这些信息加密后发送至黑客的 C&C 服务器。

2. 水利行业

2000 年，位于澳大利亚昆士兰州的马卢奇污水处理厂发生一起系统非法入侵并导致污水未经处理便排入河流的恶性事件。这起事件的起因是一名工程师应聘澳大利亚的一家污水处理厂多次被拒后产生仇恨，于是远程入侵该厂污水处理控制系统，前后三个月的时间，控制了 150 个污水泵站，最后导致共计 1000 立方米的污水排入河流，严重影响了当地的生态环境。

2001年，俄罗斯黑客入侵美国伊利诺伊州斯普林菲尔德市的公共供水网络系统，通过连续开关水泵阀门，导致水泵破坏，继而影响到数千家庭的供水保障，此次事件的原因归结于一家公司的SCADA软件，黑客通过攻入这家公司的SCADA系统，然后获取到供水系统的用户名和密码，进而侵入了供水网络系统。

3. 交通行业

2011年7月10日，我国京沪高铁某段线路出现接触网故障。经过检测、抢修、修复，最终发现本次事件并不是一般的雷击物理破坏所致，而很有可能遭遇到了恶意软件入侵。提取出的本次入侵电网控制系统的“蠕虫”病毒，经过国家计算机网络与信息安全管理中心检测发现，此病毒与2010年的“震网”类似，其功能主要是记录正常电网电压数据，而后改变电压，却将正常数据发至监控设备处，使得报警和监控全部失效。

2012年11月，深圳地铁2号线、5号线多趟列车多次发生故障，紧急停运。后现场验证表明，由于地铁运营采用的基于无线通信的列车自动控制系统(Communication-Based Train Control，CBTC)所使用的信号是公用2.4GHz频段，车上乘客的移动便携式Wi-Fi路由器可能会与CBTC地铁信号发生相互干扰。这无疑暴露了地铁系统的一大安全隐患。

2015年6月21日，波兰航空公司的地面操作系统遭受黑客入侵，导致系统瘫痪，无法执行新的飞行任务，致使预定航班无法出港，至少10个班次的航班被取消，1400多名乘客滞留肖邦机场。

4. 制造行业

2005年，美国有13家汽车工厂由于感染“Zotob”蠕虫而被迫关闭，50 000条生产线工人被迫停止工作，损失超过140万美元。“Zotob”通过利用微软发布的MS05-39即插即用中的安全漏洞，致使系统频繁重启，并预留下后门，阻止安装在系统中的反病毒软件升级。此外，该蠕虫还会通过445端口进行传播。

2017年6月，网络安全公司Trend Micro通过对ABB、三菱、川崎等公司的机器人进行安全测试发现，这些公司生产的工厂机器人的网络安全机制非常薄弱，弱口令问题十分常见。此外，这些工厂机器人系统大多仍使用过时的系统，而且工厂机器人的IP地址甚至是完全公开的。技术人员一般都是通过远程连接、电脑或手机发送指令等方式来控制工厂机器人。

5. 近两年重大安全事件

(1) 乌克兰停电事件

2015 年 12 月 23 日,乌克兰电网系统被黑客入侵,导致 Lvano-Frankivsk 地区 8 万人遭遇长达 6 个小时的停电。此次事件经乌克兰电视台、英国路透社及美国各大媒体相继报道并认定此次事件由俄罗斯黑客所为。后经调查发现,确认停电事故是一起网络攻击事件。攻击者使用附带恶意代码的邮件渗入电网工作站系统,并植入“Black Energy”恶意软件,由此获得对发电系统的远程接入和控制能力。

“Black Energy”最早于 2007 年就已经在俄罗斯地下网络中流通,起初,该恶意软件用于在 DDoS(Distributed Denial of Service, 分布式拒绝服务)攻击中创建僵尸网络,发送垃圾邮件,盗取银行凭证等。在后继的几个版本中,“Black Energy”新增了两个更加强大的功能,即利用 rootkit 技术在目标机上隐身,利用 killdisk 组件来破坏电脑上的数据,并以随机数据覆盖源文件,使电脑无法重启。而在乌克兰停电事件之前一个月的乌克兰大选中,多家新闻媒体被黑且被永久删除大量视频材料和文档资料,也是“Black Energy”导致的。

(2) 美国遭遇大规模的 DDoS 攻击

2016 年 10 月 21 日,美国最主要的 DNS 服务商 Dyn 宣布自己遭受了一次大规模的 DDoS 攻击,导致美国东海岸的 Twitter、CNN、亚马逊、Yelp 等数百家公司均无法访问,媒体将此次事件形容为“史上最严重的 DDoS 攻击”。Dyn 通过追查攻击来源,发现攻击来自 1000 万个 IP 的物联网僵尸网络,其中部分来源于 Mirai 僵尸网络。

此次大规模 DDoS 攻击,让世人见识到物联网的僵尸网络核弹般的破坏能量。网站应当做好相应的应急预案,云服务提供商应具备抵抗 DDoS 攻击的机制,物联网制造商应当保障对其产品的安全,而不是只关注其可用性,用户也要注意使用操作规范。

1.3　攻击动机与方式

目前,关键基础设施的典型体系架构主要包括现场设备层、现场控制层、系统运行管理层和企业管理层。现场设备层包括被控物理设备、传感器和执行器。现场控制层包括可编程逻辑控制器 PLC、分布式控制系统 DCS、远程终端单元 RTU 等工业控制器和数据采集与监控 SCADA、历史数据服务器、OPC 服务器、

工程师站和操作员站等系统运行状态监测系统和设备。生产系统运行管理层包括制造执行系统 MES、产品数据管理 PDM、生产信息管理系统 PIMS 和产品生命周期管理 PLM 等系统。企业管理层包括企业资源管理 ERP、企业管理系统、打印服务器、电子邮件系统、电子商务服务器、门户及 OA 系统等企业管理系统和软件。不同领域的基础设施可只包括其中的部分设备和系统。

关键基础设施中的系统之前大多处于专用网络中，或者控制层网络和企业网络处于物理隔离状态。但是，为了促进工业化和信息化融合发展，提高系统运行效率，关键基础设施中的现场设备和系统逐渐接入企业网或其他公共网络，现场控制设备或组件也逐渐朝着网络化和智能化方向发展演进。由于关键基础设施中的设备和系统在设计之初往往缺乏高效的信息安全防护或修复措施，这些设备和系统一旦接入企业网或其他公共网络，就势必会面临严重的信息安全威胁。近年来国际或美国发生的一系列关于关键基础设施的安全事件也有力地证明了这一点。工业控制系统是关键基础设施的核心组成部分，SCADA、DCS、PCS、PLC 等现场控制层系统已经成为网络攻击的首要目标。

1. 攻击动机

攻击者对这些关键基础设施（尤其是工业控制系统）发起网络攻击的动机主要包括政治、商业、恐怖活动三类因素。政治动机是指当国与国之间发生网络对抗时，由敌对国家支持并发起的针对另一国家信息基础设施的攻击。敌对国家企图通过对关键信息基础设施的破坏来扰乱对方国家和社会的正常运转，引发公民恐慌和社会动乱。商业动机是指商业组织受商业利益驱使，窃取基础设施系统和设备的商业机密数据，进而获取自己的商业价值。恐怖主义者通过对国家基础设施的有组织、有预谋的物理或网络攻击，实现其破坏社会稳定团结和经济建设的目的。

2. 工业控制系统存在的信息安全威胁

理解关键基础设施中的工业系统和网络面临的安全威胁、脆弱性问题及相关的攻击向量，对于建立有效的安全应对策略来说是至关重要的。总的来说，工业控制系统面临着外部网络、内部网络、移动介质和人员误操作四方面安全威胁。

（1）外部网络安全威胁

当控制层或系统运行管理层网络由封闭的专网专用业务网络接入开放的互联网后，在实现互联互通的同时，也可能会将互联网中的病毒、蠕虫等安全威胁从外部网络引入控制系统网络。此外，攻击者还可以从外部网络通过黑客技术

或钓鱼渗透到企业管理网络、控制层或系统运行管理层网络。此外,控制系统中的一些无线通信环节可能会被攻击者作为发起攻击的跳板。这些无线通信的交互协议在设计之初往往只关注了时效性,没有考虑信息安全防护,因此攻击者很容易攻破这些无线通信,并以此作为发起进一步深入攻击的切入点。因此,由于控制层或系统运行管理层的设备和系统在设计之初往往缺乏高效的信息安全防护或修复措施,这些设备和系统面临着严峻的外部网络安全威胁。

(2) 内部网络安全威胁

在现场设备层、现场控制层或系统运行管理层的设备或系统中,可能会被厂家或运维人员有意植入一些用来监测这些设备和系统运行状态、收集数据库数据的后门程序或通信通道。这些后门程序或通信通道也有可能会被攻击者当作从内部网络实施主动攻击的入口。这也就引入了内部网络安全威胁。

(3) 移动介质安全威胁

工业生产环境中的软件升级和数据导出与备份工作往往都会用到移动介质。但是对于移动介质的安全管理普遍缺乏有效的监督与控制机制,无法保证工业生产环境下的移动介质专盘专用。例如运维或内部员工将插入过连接互联网设备的优盘直接接入控制层或系统运行管理层的设备,进而导致设备感染病毒或木马程序。虽然控制层或系统运行管理层的设备中也有专门的杀毒软件,但是这些杀毒软件却难以应对各种病毒或木马新型变种,因此,工业生产过程中也面临着严峻的移动介质安全威胁。

(4) 人员误操作安全威胁

内部和外部人员由于缺乏专门适用于控制系统的网络安全技术,在远程或现场运维过程中,可能会发生不恰当的网络安全操作,从而导致设备或系统发生物理或网络故障。这也是一个不容忽视的安全隐患问题。

3. 攻击方式

对应于上述工业控制系统中存在的信息安全威胁,攻击者的攻击途径包括从外部网络、内部网络和移动介质入手等方式。此外,攻击者还可能渗透系统运行环境设备(如视频监控网络摄像头),通过利用这些设备的漏洞来将其变成为己所用,进而发起对工控网络的攻击。

攻击者的攻击方式一般包括侦查、扫描、枚举、渗透或扰乱、控制等。首先,攻击者通过网络扫描和探测,确定工控资产类型、转换时间安排表、系统额外的接入点,以此来侦查找到系统入侵的入口;其次,攻击者通过对常用端口和服务的进一步搜索识别出常见工控设备;然后,攻击者再通过枚举方式在工控系统中

的人机接口(Human Machine Interface,HMI)、历史数据库等设备中建立据点;最后,攻击者通过渗透(如由目标 HMI 渗透进入目标可编程逻辑控制器(Programmable Logic Controller,PLC))、控制(如在系统上通过成功安装和执行恶意代码来长期控制系统)和扰乱(如通过防火墙上开发端口的恶意扫描引起的泛洪攻击或欺骗攻击合法通信,注入异常流量,造成 DoS 攻击)等方式来达到破坏系统或设备的目的。

1.4 美国政府安全政策

美国自克林顿政府时期,就已经开始关注关键基础设施安全问题,并发布了首个关于关键基础设施防护的行政令。随后,小布什政府颁布了具体保护计划和国土安全法,并建立了国土安全部来专门负责国土安全事务。奥巴马上台后,继续加强了保护关键基础设施的力度。特朗普政府也通过签署网络安全行政令的形式,在联邦网络、关键基础设施和国家三个方面,规定了增强网络安全的措施。表 1-1 总结了美国近几届政府在关键基础设施方面的典型政策和文件。

表 1-1 美国近几届政府典型政策、战略计划一览表

时间	政府	名称	主要信息
1996.7.15	克林顿政府	第 13010 号行政令《关键基础设施防护》	规定了关键基础设施 8 个领域范围
1998.5.22	克林顿政府	第 63 号总统决策指令《关键基础设施防护》	明确了关键基础设施相关责任部门
2001.10.16	小布什政府	第 13231 号行政令《信息时代的关键基础设施防护》	成立"总统关键基础设施保护管理委员会",并要求委员会定期提出发展政策和建议
2002.11.25	小布什政府	《国土安全法》	成立国土安全部,负责关键基础设施安全工作
2002.7.16	小布什政府	《国土安全国家战略》	遏制恐怖袭击活动,提高国土安全防御能力,保护关键基础设施和重要资产
2003.2	小布什政府	《关键基础设施和重要资产物理保护国家战略》	明确了政府和私营机构在保护关键基础设施方面的不同职责

续表

时间	政府	名称	主要信息
2006.6	小布什政府	《国家基础设施保护计划》	为政府和私营机构提供关键基础设施保障的实施框架
2013.2.12	奥巴马政府	第 13636 号行政令《提高关键基础设施的网络安全》	明确要求国土安全部采取措施推进政企合作，建立网络安全信息共享机制
2013.2.12	奥巴马政府	第 21 号总统政策指令《提高关键基础设施的安全性和恢复力》	确定了通信、金融服务、信息技术等 16 类关键基础设施行业
2014.2.12	奥巴马政府	《提高关键基础设施网络安全的框架规范》	美国政府首次提出的国家级信息安全指导规范，自 2013 年以来的第一个较全面的基础性指导文件
2015.12.18	奥巴马政府	《2015 年网络安全法案》	美国在网络安全信息共享方面的一部较为完备的法律
2016.2.9	奥巴马政府	《网络安全国家行动计划》	推动国家网络现代化、安全化工作，提出了一系列举措
2017.5	特朗普政府	网络安全行政令《增强联邦网路和关键基础设施的网络安全》	在联邦网络、关键基础设施和国家三个方面，规定了增强网络安全的措施

1. 克林顿政府时期政策

1996 年 7 月 15 日，克林顿颁布了第 13010 号行政令《关键基础设施防护》[17]。该行政令宣布成立总统关键基础设施保护委员会。委员会包括一名主席和数名委员。主席是由总统任命的联邦政府以外的一名全职人员。委员由财政部、司法部、国防部、商业部、交通部、能源部、中央情报局、联邦应急管理局、联邦调查局和国家安全局等部门领导各自推荐的 1～2 名员工组成。委员会还设立了指导委员会、主管委员会和咨询委员会。指导委员会定期审阅委员会工作进展报告。经审阅后的报告，指导委员会批准提交给主管委员会。咨询委员会

是由关键基础设施私营部门的专家组成，负责向委员会提供咨询和建议服务。该行政令限定了关键基础设施范畴包括电信、电力、天然气石油存储和运输、银行和金融、交通、水利供应、应急服务（如医疗、警务、火警和救援）及其他保障政府持续运作的8类系统。

1998年5月22日，克林顿颁布了第63号总统决策指令《关键基础设施防护》[18]。该指令在明确关键基础设施范畴的基础上，进一步明确了财政部、司法部、国防部、商业部、交通部、能源部、中央情报局、联邦应急管理局、联邦调查局和国家安全局等相关责任部门的任务分工。此外，该指令还制定了一个国家目标，即在2003年之前，联邦政府及相关责任部门、州和地方政府、私营部门应该各司其职，美国应该拥有保护国家基础设施的能力。

2. 小布什政府时期政策

2001年10月16日，小布什政府颁布了第13231号行政令《信息时代的关键基础设施防护》[18]，宣布成立总统关键基础设施保护管理委员会，并要求委员会定期针对关键基础设施保护工作提出发展政策和建议。委员会与国土安全部一起，为美国行政管理和预算局提供关键基础设施安全项目预算建议。此外，委员会还会定期督导美国国家科学基金会、能源部、交通部、环境保护局、商业部、国防部等单位开展关键基础设施相关项目。

2002年11月25日，小布什总统在白宫签署了《国土安全法》[20]，宣布将原来隶属于联邦调查局、国防部、商业部、能源部等机构的相关单位进行整合和重组，重新组建了一个主要负责国土安全事务的联邦行政部门，即国土安全部。国土安全部的主要职责包括，防止发生针对关键基础设施的恐怖袭击事件，加强其安全防范能力，管理和保护边境安全，落实和监管移民法规，保卫网络空间安全，增强自然灾害应对能力。

2002年7月16日，小布什政府发布了《国土安全国家战略》第一版[21]。该战略的目的是动员和组织联邦政府、州和地方政府、私营部门和美国公民一起遏制恐怖袭击活动，提高美国国土安全防御能力，保护关键基础设施和重要资产并提高其应急响应和恢复能力。该战略归纳了6个关键任务：建立恐怖主义活动信息情报搜集和预警系统，关注边境和交通安全，开展国内反恐行动，保护关键基础设施和重要资产，预防化学、生物和核等武器威胁，应对和响应突发事件。随后，2003年2月，小布什总统针对保护关键基础设施和重要资产任务，发布了《关键基础设施和重要资产物理保护国家战略》[22]，该战略将农业和食品、水利、公共健康、应急服务、国防工业基础、电信、能源、交通、银行和金融、化学工业和

危险材料、邮政和航运等设施作为关键基础设施，将国家古迹和建筑、核电站、大坝、政府设施、商业设施作为重要资产。该战略针对保护关键基础设施和重要资产，强调了面临的挑战问题，并给出了解决这些问题的技术路线。

2006 年，国土安全部发起了《国家基础设施保护计划》[23]。该计划的目标是通过加强对国家关键基础设施和重要资产的保护，建立一个物理上、信息网络上更安全以及故障恢复能力更强的美国，以此来阻止、减缓或消除由恐怖袭击所带来的蓄意破坏影响。加强国家在袭击、自然灾害或突发等事件中的预防、及时响应和快速恢复的能力。为了实现这些目标，该计划要求实现以下 4 个具体目标：共享恐怖袭击和其他灾难危害事件的信息，实现一个长远规划的风险管理系统，最大化重要资产的使用效率。

3. 奥巴马政府时期政策

2013 年 2 月 12 日，奥巴马政府同时颁布了第 13636 号行政令《提高关键基础设施的网络安全》[21]和第 21 号总统决策指令《提高关键基础设施的安全性和恢复力》[20]。第 13636 号行政令旨在指导行政部门设计一个技术中立的网络安全框架；促进和鼓励相关单位采取网络安全防护措施；增加网络威胁信息共享的数量，并提高信息共享的实时性；在开展关键基础设施安全防护工作时，要求政府保障公民的隐私和自由权利；利用现有法规来规范和改进网络安全。第 21 号总统决策指令代替了原来的第 7 号总统决策指令，明确指出了化学、商业设施、通信、关键制造、大坝、国防军工、应急服务、能源、金融服务、食品和农业、政府设施、公共卫生、信息技术、核反应堆材料和废物、交通、城市供水和废水处理系统 16 种关键基础设施行业。该总统政策指令旨在督促相关部门建设一种物理和网络全方位安全态势感知能力，要求行政部门和主管部门分析、理解不同基础设施行业系统故障和安全事件的级联后果，评估和完善公共部门和私营部门之间的合作关系及安全事件信息共享机制，不断更新发布关键基础设施安全保护计划和项目。

在第 13636 号行政令和第 21 号总统决策指令的指导要求下，3000 多个信息安全专家在全国开展了一系列工业安全研讨会，共同讨论了 10 个月后，由美国国家标准与技术研究院起草了《提高关键基础设施网络安全的框架规范》(简称《规范》)[26]的第一个版本。2014 年 2 月 12 号，美国白宫公布了这一规范。该规范是自美国启动保护关键基础设施信息安全工作以来发布的第一个较全面的基础性指导文件。《规范》制定了一个基于风险评估方法来管理网络安全风险的安全框架。该框架包括识别、保护、检测、响应和恢复五个方面，可以帮助相关组

织机构来识别安全风险，实施和改进网络安全实践。

为了进一步加强网络安全法律、法规保护力度，2015 年 12 月 18 日，奥巴马签署了《网络安全信息共享法案(2015)》[27]，并将其标注为《2015 年网络安全法案》。该法案不仅将国土安全部作为网络安全信息共享的枢纽，还赋予了网络服务提供商更高的网络监控权利，是美国目前在网络安全信息共享方面的一部较为完备的法律。此外，该法案第 208 条专门对“多重并发的关键基础设施网络事件”给出了法律规范。

除了通过立法来促进改善国家网络安全以外，奥巴马政府还在 2016 年 2 月 9 日推行了《网络安全国家行动计划》，从建立国家网络安全促进委员会、提升国家整体网络安全水平、阻止/劝阻并破坏网络空间恶意行为、提高网络安全事件响应能力、保护个人隐私、加大网络安全研发投入等方面来全面推动美国网络现代化、安全化工作。其中，在提升国家整体网络安全水平方面，该计划明确指出，要增强关键基础设施的安全性和恢复力。

4. 特朗普政府时期政策

2017 年 5 月 11 日，特朗普总统签署了网络安全行政令《增强联邦网路和关键基础设施的网络安全》，在联邦网络、关键基础设施和国家三个方面，规定了增强网络安全的措施。在关键基础设施网络安全方面，该项行政令要求应遵照奥巴马政府颁布的第 21 号总统决策指令所规定的关键基础设施行业进行安全评估，并于 180 日内提交其网络安全风险评估报告，今后每年度评估一次并更新报告。

1.5 本书组织

本书共 6 章，首先给出了关键基础设施安全概述，然后分别介绍了美国国土安全部、能源部、国家标准与技术研究院、国家科学基金会、国防高级研究计划局在关键基础设施领域开展的相关工作。本书按照以下结构来安排：

第 1 章关键基础设施安全概述。首先，介绍了中国和美国对关键基础设施的解释和定义，基于这些定义，给出了本书的定义。然后，简述了近年来发生的典型安全事件，并分析了这些安全攻击的动机和模式；最后针对这些安全攻击事件，总结了美国近几届政府作出的应对政策。

第 2 章介绍了美国国土安全部的相关工作。首先，介绍了国土安全部基本情况及其职责。其次，详细介绍了“网络风暴”系列演习。然后，介绍了工业控制

系统网络应急响应小组的主要职责及其网络安全报告内容。最后介绍了国土安全部开展的重要项目。

第 3 章介绍了美国能源部的相关工作。首先,介绍了能源部及其国家实验室的基本情况。然后,介绍了能源部发布的能源行业控制系统安全防护技术路线。最后,介绍了能源部最为著名的国家 SCADA 测试床项目及其具体承担项目情况。

第 4 章介绍了美国国家标准与技术研究院的相关工作。首先,介绍了国家标准与技术研究院的基本情况及其典型项目。然后,详解了该机构发布的两个关于关键基础设施的重要文件,即提高关键基础设施网络安全的框架规范和工业控制系统安全指南。最后,介绍了该机构开展的典型网络安全性能测试床。

第 5 章介绍了美国国家科学基金会的相关工作。首先,介绍了国家科学基金会基本情况。然后,介绍了在关键基础设施安全方面开展的研发项目。最后,介绍了基础设施安全项目中的所有课题情况。

第 6 章介绍了美国国防高级研究计划局的相关工作。首先,介绍了国防高级研究计划局基本情况。然后,介绍了网络空间项目 Plan X 项目。最后,给出了本章小结。

参考文献

[1] 中国政府网. 中共中央关于全面深化改革若干重大问题的决定.(2013 年 11 月 12 日中国共产党第十八届中央委员会第三次全体会议通过). http://www.gov.cn/jrzg/2013-11/15/content_2528179.htm

[2] 新华网. 中央网络安全和信息化领导小组第一次会议召开 习近平发表重要讲话. http://www.cac.gov.cn/2014-02/27/c_133148354.htm

[3] 新华社. 习近平总书记在网络安全和信息化工作座谈会上的讲话. http://www.cac.gov.cn/2016-04/25/c_1118731366.htm

[4] 新华社. 习近平主持召开国家安全工作座谈会. http://news.xinhuanet.com/politics/2017-02/17/c_1120486809.htm

[5] 中国政府网. 李克强作政府工作报告(文字实录). http://www.gov.cn/guowuyuan/2016-03/05/content_5049372.htm

[6] 新华社. 李克强:抓住"一带一路"机遇 推进能源基础设施互联互通. https://www.yidaiyilu.gov.cn/xwzx/xgcdt/2610.htm

[7] 中华人民共和国环境保护部. 新《中华人民共和国节约能源法》(2016 年 7 月修订). http://www.zhb.gov.cn/gzfw_13107/zcfg/fg/xzfg/201610/t20161008_365106.shtml

[8] 国务院办公厅. 国务院办公厅关于开展重大基础设施安全隐患排查工作的通知.(国办发〔2007〕58 号). http://www.gov.cn/xxgk/pub/govpublic/mrlm/200803/t20080328_32591.html

[9] 国务院办公厅. 国务院关于大力推进信息化发展和切实保障信息安全的若干意见.(国发〔2012〕23 号). http://www.gov.cn/zwgk/2012-07/17/content_2184979.htm

[10] 中国政府网.《国务院关于加强城市基础设施建设的意见》.(国发〔2013〕36 号). http://www.scio.gov.cn/32344/32345/32347/33173/xgzc33179/Document/1442976/1442976.htm

[11] 中华人民共和国工业和信息化部. 工业和信息化部关于加强电信和互联网行业网络安全工作的指导意见.(工信部保〔2014〕368 号). http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057729/c3644576/content.html

[12] 中华人民共和国工业和信息化部. 关于加强工业控制系统信息安全管理的通知.(工信部协[2011]451 号)http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057656/n3057661/c3595372/content.html

[13] 中华人民共和国网络安全法.(2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过). http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm

[14] 中国人大网. 国家互联网信息办公室. 国家网络空间安全战略. http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

[15] 中国网信网. 全国范围关键信息基础设施网络安全检查工作启动. http://www.cac.gov.cn/2016-07/08/c_1119185700.htm

[16] 国家互联网信息办公室. 国家互联网信息办公室关于《关键信息基础设施安全保护条例(征求意见稿)》公开征求意见的通知. http://www.cac.gov.cn/2017-07/11/c_1121294220.htm

[17] Executive Order 13010. Critical infrastructure protection. 1996. http://fas.org/irp/offdocs/eo13010.htm

[18] Presidential Policy Directive(PPD)-63. Critical infrastructure protection. http://fas.org/irp/offdocs/pdd/pdd-63.htm

[19] Executive Order 13231. https://www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10-16-initial.pdf

[20] Department of Homeland Security. Homeland Security Act of 2002. https://www.dhs.gov/homeland-security-act-2002

[21] Department of Homeland Security. National strategy for homeland security. https://www.dhs.gov/publication/first-national-strategy-homeland-security

[22] Department of Homeland Security. The physical protection of critical infrastructures and key assets. https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

[23] Department of Homeland Security. National infrastructure protection plan. https://www.dhs.gov/national-infrastructure-protection-plan

[24] Executive Order 13636. Improving critical infrastructure cybersecurity. 2013. http://fas.org/irp/offdocs/eo/eo-13636.htm
[25] Presidential Policy Directive (PPD)-21 Critical infrastructure security and resilience. https://fas.org/irp/offdocs/ppd/ppd-21.pdf
[26] NIST. Framework for improving critical infrastructure cybersecurity. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
[27] Cybersecurity Information Sharing Act of 2015. https://www.dni.gov/index.php/ic-legal-reference-book/cybersecurity-act-of-2015
[28] FACT SHEET: Cybersecurity National Action Plan. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan
[29] The White House. Presidential executive order on strengthening the cybersecurity of federal networks and critical infrastructure. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

第 2 章　美国国土安全部

本章首先总结分析了美国国土安全部组织的“网络风暴”系列演习的内容和成果，然后整理了国土安全部工业控制系统网络应急响应小组近 8 年的年度网络安全报告，并调研了国土安全部近年来在关键基础设施安全方面部署的典型项目。

2.1　国土安全部职责

“9・11”事件发生之后，为了应对恐怖袭击活动，美国小布什总统于 2002 年 11 月 25 日签署了《国土安全法》，宣布成立国土安全部。美国政府将原来隶属于联邦调查局、国防部、商业部、能源部等机构的相关单位进行了整合和重组，重新组建了一个主要负责国土安全事务的联邦行政部门，即国土安全部。国土安全部的核心职责包括 5 个方面：防止发生恐怖袭击事件和加强安全防范能力，管理和保护边境安全，落实移民法规和监管，保卫网络安全，增强自然灾害应对能力。

针对上述五个职责，国土安全部设立了国家保护与计划司、管理司、科学技术司，政策、法律顾问、健康事务、公共事务、国内核探测、情报分析等办公室，另设秘书长和副秘书长、行政秘书和军事顾问等职位。此外，国土安全部还设置了美国海关和边境保护、美国公民和移民服务、美国移民和海关执法、美国海岸警卫、联邦应急管理、美国特勤和美国交通安全管理等机构。国土安全部的组织架构如图 2-1 所示。

2.2　网络风暴演习

“恐怖袭击”和“网络威胁”是自“9・11”事件之后美国面临的首要国家安全威胁，“关键基础设施”是主要攻击目标。因此，为了提高美国关键基础设施系统的安全防范和应急响应能力，国土安全部的国家网络安全局（National Cyber Security Division，NCSD）在 2006 年组织开启了“网络风暴”（Cyber Storm，CS）

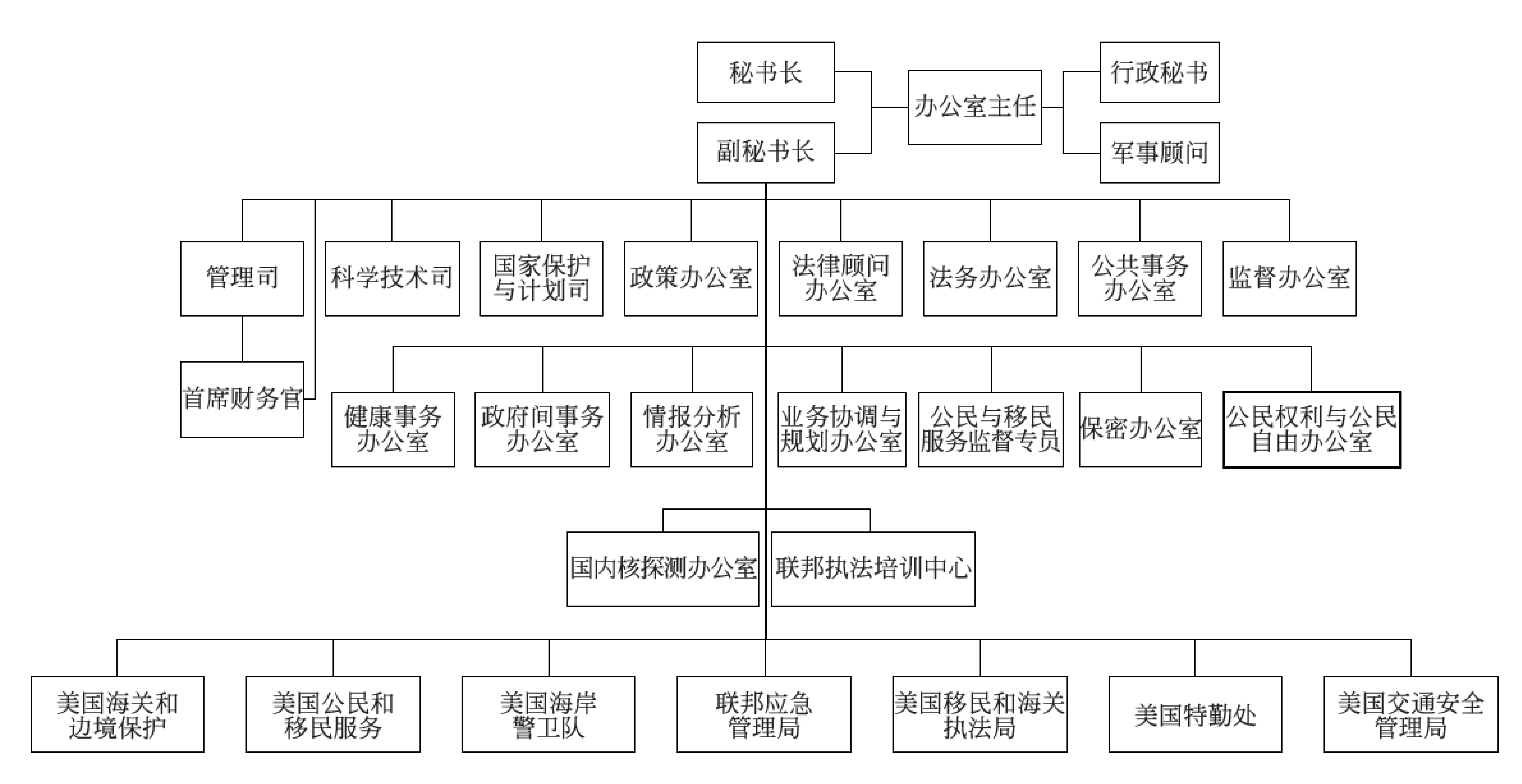


图 2-1　美国国土安全部组织架构[1]

系列演习[2]。该演习是第一次由美国政府主导的大规模国家级网络安全演习。美国公共部门、私营部门、国际机构、公司等共计 100 多个单位参与了本次演习的筹备和实施工作。“网络风暴”系列演习的主要目的是：①检验网络安全应急预案是否合理，预案是否成熟；②基础设施使用者和厂商之间、政府部门之间网络安全信息共享是否充分、及时；③应急团队对网络攻击的补救用时、损失代价等最终处理效果是否满足既定目标。

与一般的攻防比赛不同，“网络风暴”系列演习侧重于考察参演单位在网络攻击情况下的协调应急能力，而不是将选拔技术人才作为演习的主要目标。演习主要关注如何处理好公共部门和私营企业之间的关系以及联邦政府和州、地区及各国政府之间的协同关系。例如，“网络风暴Ⅰ”演习旨在提高联邦、州、五眼联盟政府以及私营部门之间协同应对网络空间重大攻击事件的应急响应能力。该演习在预先准备好的封闭环境中，模拟了一个复杂的网络攻防场景。攻方针对能源、信息系统、金融和交通等行业的关键基础设施发起攻击，破坏联邦政府及五眼联盟参演网络；守方负责监测、搜集攻击信息、制定实施应急响应预案以及采取安全保护措施。演习通过发现攻击、共享信息、协同采取网络安全防护技术等方式来在不同层面演练参演单位之间的协同应急响应能力。

迄今为止，“网络风暴”系列演习已经开展了 5 次。通过这些演习，参演人员发现了在网络安全应急响应过程中存在的诸多问题。针对暴露出来的问题，应急响应共同体通过不断地修订应急预案、加大信息共享力度，逐渐提高了在关键基础设施遭受恐怖袭击和网络攻击时的应对能力。

2.2.1　网络风暴 I

1. 基本情况

- 演习时间：2006.2.6—2006.2.10
- 组织单位：国土安全部国家网络安全局
- 演习目的：针对关键基础设施发生的重大网络安全事件，提升联邦、州、国际政府等公共部门之间及其与信息技术、电信、能源和交通等私营部门之间的应急响应协作能力。
- 参演方：①五眼联盟*国家——英国、美国、加拿大、澳大利亚和新西兰；②国土安全部、商务部、国防部、国家安全局、能源部、国务院、交通部、财政部、美国联邦存款保险公司、纽约联邦储备银行、司法部、卫生及公共服务部、中央情报局、行政管理和预算局、国家安全委员会、国土安全委员会、美国红十字协会、多州信息共享和分析中心、密歇根州政府、蒙大拿州政府、纽约州政府等联邦或州公共部门；③1 个银行和金融公司、11 个信息技术公司、北美电力可靠性委员会、7 个电力公司、2 个民航公司、加拿大空域管制机构、4 个信息共享和分析中心等私营部门。
- 演习场所：具体演习场所共 60 余处，指挥部设在华盛顿。

2. 演习目标

演习的目的是通过演练网络攻防和安全事件响应过程，评估参演单位的网络安全应急响应能力和信息共享协作能力。通过演习发现安全事件信息共享和单位之间沟通协作等工作中存在的障碍，制定或修改网络安全应急响应预案，规范共同途径和方法，提高应急响应共同体的工作效率，加强安全防范与应对能力[3]。“网络风暴 I ”演习手册规定了本次演习的 8 个目标：

(1) 通过创建国家网络响应协调组（National Cyber Response Coordination Group，NCRCG）和跨部门事件管理组（Interagency Incident Management Group，IIMG）来负责网络空间安全事件应急响应中的协调和管理工作，演练不同部门之间的安全事件处理、沟通与决策。

(2) 演练不同国家政府之间及联邦政府和州政府之间的沟通协调和事件响应能力。

---

* 五眼联盟国家指英国、美国、加拿大、澳大利亚和新西兰。

（3）找出阻碍实施网络安全措施的政策或体制问题。

（4）建立公共和私营部门之间有效的沟通渠道，提高网络安全事件响应和恢复协调效率，明确关键信息共享的路径和机制。

（5）为了促进关键基础设施主管或运营单位和企业之间的信息沟通，应明确公共和私营部门之间沟通信息的过程和程序。

（6）明确基础设施的网络物理相互依赖关系对现实世界经济和政治的影响。

（7）提高民众对重大网络安全事件在经济和国家安全方面影响的关注度。

（8）重点关注如何提高网络事件响应和恢复的能力，研发相关可用工具和技术。

3. 演习范围及场景

"网络风暴Ⅰ"演习范围设定在能源、交通、IT/通信三个领域。演习规划团队预先建立一个封闭安全的网络环境，消除演习系统的任何外部干扰因素，在此封闭环境中执行所有模拟攻击和练习。因此，演习对任何真实世界的关键基础设施都无损害。所有演习场景虽然都是基于假设且绝对有可能发生的，但并不能将它们作为未来与恐怖袭击或网络攻击事件的预言。

本次演习仿真了复杂的网络攻击活动，设计这些场景的目的是要突出网络系统与物理基础设施间的关联性，并检验政府、公共部门和私营部门之间的协调和沟通能力。演习旨在提高参与者应对网络战的响应能力，同时帮助其充分理解、分析和评估关键网络元素的作用。基于模拟的网络元素，具体演习场景包括：破坏能源和交通基础设施的网络攻击；破坏联邦、州与国际政府的IT/通信系统的正常运转，以此来摧毁政府的公众信任度。演习参与者通过以下过程来实际演练：

（1）识别所有沟通渠道，并有效地使用这些渠道来交流分析攻击行为。

（2）将一系列相互关联的事件进行整理汇总，以此作为一个严重的安全威胁问题，提交给国家网络响应协调组处理。演练国家网络响应协调组与跨部门事件管理组之间的协调沟通关系。

（3）通过设定、执行和调整应急预案，演练美国联邦、州及国际政府等公共部门和能源、交通、IT/通信单位等私营部门之间的信息共享和协作能力。

4. 演习成果

"网络风暴Ⅰ"是一次复杂的多国家、跨部门网络安全演习，是美国国家和国

际社会关键基础设施网络安全事件和恐怖袭击应急响应工作的一个里程碑。演习实现了培训与关键基础设施相关的单位和个人的应急能力，检验不同国家、部门之间的协作沟通能力等方面的既定演习目标。具体地，本次演习取得了 7 个重要成果。

（1）跨国家、跨部门协调能力

本次演习中，国家网络响应协调组（NCRCG）与跨部门事件管理组（IIMG）积极协调合作，评估了国家关键基础设施的安全影响因素，定义了国家安全和经济利益所面临的威胁，提升了国土安全预警系统的安全水平。但是，在对网络攻击或其他威胁进行响应时，二者仍需要进一步增强合作力度，有效提升系统的安全评估水平和预警准确度。

对于网络应急活动来说，信息的双向流动是关键。更大范围内的信息共享，可为国家和国土安全进行关键决策，提供更符合情况的指导帮助。在演习中，美国电脑警备小组（United States Computer Emergency Readiness Team，US-CERT）服务作为应急响应信息的汇总和过滤者，对 DHS 和 NCRCG 的核心和外围机构提供应急信息。这一角色至关重要，对 DHS 和 NCRCG 获知安全态势情报至关重要。演习发现，US-CERT 在支持 NCRCG 方面表现不错，但同时，在运行信息过滤方面，它们的峰值处理能力却不太尽如人意。因此，US-CERT 今后需要考虑如何利用点到点分布式方式来提高海量安全事件信息处理速度和效率。此外，在面对重大灾害或一系列事件时，错误的媒体信息可能会导致公众恐慌，而且不正确的媒体信息可能比敌人的攻击所带来的损害会更大。因此，演习发现，无论信息源头在哪里，都要建立一个清晰的公众报道和信息公布渠道，准确并及时地将易被民众理解的重要信息发布出去。

参与演习的同盟国参与者发现，需要仿照美国 IIMG 和 NCRCG，明确并组织建立和自身国家相适应的职能清晰、结构合理的应急响应处理组织。从而有利于各国在现实场景下遭遇网络攻击时，能够实施更有效的应急响应行动。

（2）不断完善响应过程、风险评估、角色和责任，制定备份通信方案

对于许多参与者来说，由于之前未曾碰到过类似网络安全的事故，缺乏完备的标准化响应过程和预案，当需要与其他参演机构试图建立信任和伙伴关系时，他们根本无法确认不同机构应当承担的角色和责任。因此，在下一次风暴演习之前，各参与国和组织机构都应针对这次演习中所暴露的问题一一排查，从风险评估到各组织机构的协作并明确各自角色责任，最后形成一个标准化响应流程。

此外，由于网络事件的响应活动对通信系统的高度依赖性，通信系统往往会成为敌方网络安全攻击的主要对象。演习发现，除上述需要不断完善的部分之

外，更需要针对网络安全事件导致通信中断的情况事先制定备份通信或是快速恢复的通信方案。

（3）多个事件中公共和私营部门的协作，网络安全实体间的合作

即使演习中的大多数安全事件都被认为是一个个孤立的事件，但是当对演习中的安全事件之间的相互依赖性进行评估时，通常涉及多个部门和事件。如何协调多个基础设施的多个事件，以及加强公共与私营部门间的协作，这些问题对于各参与国、机构仍然是一个重大挑战。在应对多个网络安全事件时，演习凸显了建立快速安全评估和安全事件优先级快速排序或快速分类方法的重要性。

随着网络安全事件的增加，不同网络安全实体之间的协作和沟通的重要性逐渐显现出来。演习中各实体间的协调合作对于安全事件应急响应显得尤为关键。本次演习针对机构网络安全响应的能力进行了演练。多重的、同时发生的、需要协调处理的安全事件，给应急响应提出了更高的要求。针对并发的攻击，在需要协调处理的情况下，尤其是有多方面影响因素或者多个责任单位的安全事件而言，确定应急响应的优先顺序，准确整合信息以确定恰当的响应是解决网络安全事件的关键点。澄清跨部门的角色和责任，并在公众和私营部门中明确阐述安全责任及后果，可以帮助参与者更好地建立协调预防和解决办法。

（4）反复演习项目作用

反复演习将有助于参与者加强实施有组织的网络安全事件响应活动能力，熟悉划分任务角色，并不断完善应急响应政策和信息共享流程。持续开展网络安全培训、讨论交流和安全演习，对于建立不同组织之间的相互协作，加强对网络安全事件的协调响应是行之有效的办法。可信、及时的安全事件信息对于参与者制定安全响应对策来说是至关重要的。这些安全信息的获取和甄别方法也需要通过定期的安全演习来不断得到完善。

（5）应急响应和信息访问的通用框架

一个应急响应和信息访问的通用框架，可以为网络事件的相关者提供一种用以应急响应、安全评估和讨论的沟通渠道。可用的信息交流通道加强了国内与国际网络应急响应团体之间的关系。如同真实世界，网络风暴也存在时而信息匮乏时而数据过多的情况。绝大多数的演习参与者都反映，要识别精确和最新的信息源是比较困难的。针对一个单点事件往往有多重安全警报，这在演习者中容易引起混乱，难以建立一个单一的协调响应流程。因此，演习参与者们强调，单点信息将有助于建立一个应急响应和信息访问通用框架，并且有利于提高应急响应的时效性。US-CERT 提供了重要的可操作的信息，包括安全警报和技术公告。然而，仍需要进一步提高 US-CERT 公布信息的能力，使这一过程变

得更及时、安全和精确。演习参与者们认为，US-CERT 是最适合向相关组织分发实时关键信息的机构。

（6）战略通信和公共关系规划

公共信息必须作为协作应急计划和事件响应的一部分，为事件响应相关各方提供关键信息，并使公众能够采取符合自身状况的个人防护或响应行动。

对于私营单位来说，公共事务就意味着战略沟通。跨国、私营部门之间的沟通机制和公共关系一定要落实到位，这样才能在危机发生时采取有效的协调办法。此外，公共事务作为规划和响应流程的一部分也很重要，因为公共事务在建立公众安全事件应对和响应信心方面扮演着重要角色，并且也给公众和媒体提供了安全事件信息。

联邦响应措施一定要确保公共事务团队能够及时将新闻稿和准确的时况信息提供给合作组织和媒体。这些组织间的协调将保证新闻消息不会进入错误渠道，所有的联邦官员都可获得一个统一的信息用于对外公布。这一点做得成功将增加公众的信任，将把个人和企业响应错误信息的负面影响减到最小。

（7）过程、工具和技术的改进

改进的流程、工具和训练，关注的是分析网络攻击总体所产生的物理的、经济的和国家安全的影响，并将其分出不同的优先级，将会改进响应工作的质量、效率及协调工作的顺畅度。

在演习规划期间，演习参与者对监控与数据采集系统（Supervisory Control And Data Acquisition，SCADA）进行了深入的研究并发现了大量安全问题。此外，也证实了当漏洞存在要进行安全修复时存在的种种困难。此外，对于在组织间交换和共享机密信息问题，亟须开发一种能够在整个响应社区内以较低密级处理和共享关键信息的框架和流程。还需要设计能够降级/脱密的方法，从而实现与相关组织共享来自机密信息源的信息交互渠道和流程。

小结：5 个国家、60 多个地方的超过 100 个公共和私营机构、协会、公司参与了“网络风暴 Ⅰ”演习。总而言之，无论从保护关键基础设施的国家和国际网络事件响应方面，还是从公众和私营部门合作关系的利益方面看，“网络风暴 Ⅰ”都是一次重要的里程碑式演习。对参与者以及相关人员，演习达到了所制定的训练目标。多层次跨国协作应急响应能力得到了有效提升。联邦机构之间，包括情报、执法部门、军队，私营部门和政府之间，以及国际合作伙伴之间的协作和信息共享演练效果显著。本次演习检验了国家层面上的网络安全事件应急响应预案的可行性。此外，本次演习还建立起了多个政府公共组织和私营部门的合作

渠道，有利于今后开展跨部门安全事件应急响应工作。

2.2.2 网络风暴Ⅱ

1. 基本情况

- 演习时间：2008.03.10—2008.3.14
- 组织单位：国土安全部国家网络安全部门
- 演习目的：提升联邦、州、国际政府以及私营部门之间，应对网络空间重大攻击事件的应急响应能力。
- 参演方：①五眼联盟国家；②国土安全部、中央情报局、宾夕法尼亚州、弗吉尼亚州、商务部、国防部、能源部、卫生及公共服务部、司法部、国务院、交通部、情报社区事件响应中心、国家安全局、国家网络响应协调小组、加利福尼亚州、科罗拉多州、特拉华州、伊利诺伊州、密歇根州、北卡罗来纳州、得克萨斯州、田纳西河流域管理局等联邦或州公共部门；③2 个管道公司、15 个信息技术公司、3 个铁路公司、9 个信息共享和分析中心等私营部门。
- 演习场所：指挥部设在华盛顿的美国特工处。

2. 演习目标

“网络风暴Ⅱ”演习旨在改善网络事件响应共同体的能力，促进发展在关键基础设施行业中不同单位之间的合作伙伴关系，加强联邦政府和州、地区和国际层面政府伙伴之间的关系。本次演习的主要目的是检验网络响应共同体在应对全球 IT、通信、化学和交通运输领域基础设施典型行业遭受网络协同攻击时的应急响应能力。为了应对网络协同攻击，演习促使参与者从技术、行动和战略等方面进行安全事件应急响应[4]。

演习目标如下：

(1) 检验网络事件响应共同体预防和响应网络协同攻击的能力；

(2) 依照国家层面应急响应政策和程序，演练高层领导在决策过程中和不同机构之间的协调与合作；

(3) 针对网络事件态势感知、响应和恢复信息的收集和分发，检验信息共享方式和沟通渠道是否通畅；

(4) 在不损失知识产权和国家安全利益的前提下，检验跨边界敏感信息和保密信息的共享方式和过程是否恰当。

3. 演习范围及场景

“网络风暴Ⅱ”的设计目标是在应对协同网络攻击的预防、响应和恢复过程中，演练公共和私营部门的协调能力，制定并评估网络安全应急响应预案，改进网络安全环境。在网络安全事件响应时间和资源的限制条件下，演习范围主要集中于重要利益相关方进行跨行业跨部门的协调合作。

与“网络风暴Ⅰ”类似，本次演习也是在一个封闭的模拟环境下，演习参与者演练他们在 IT、通信、化工及铁路和管道交通运输行业的网络安全应急响应能力。演习集中于三个主要场景：互联网中断、通信中断和控制系统破坏。在演习过程中所有的攻击都是模拟的，对现实世界正在运行的网络没有任何影响。

4. 演习成果

本次演习按照四个既定目标开展了一系列制定、修改、执行预案的应急响应演练工作。演习取得了 5 个显著成果。

(1) 标准操作流程和建立合作关系的价值

通过本次演习发现，参演单位制定了标准操作流程和建立不同组织之间的协作关系，不仅提高了制定安全事件应急响应预案和开展应急恢复工作的效率，而且还加快了安全事件信息在网络安全应急响应共同体中的传播速度。本次演习不仅进一步细化和完善了标准操作流程，使之变得更加成熟和规范，而且还通过模拟协同网络攻击，更加强调了在攻击发生之前不同组织之间建立协作关系的重要性。

(2) 物理和网络的相互依赖性

网络安全事件能够产生物理破坏影响，物理破坏也会反作用于网络安全。物理攻击和网络攻击所导致的后果通常存在较为紧密的联系。物理攻击影响网络基础设施，网络中断可能造成严重的物理后果。通过对事件产生的所有可能后果进行分析，并据此制定响应方案，可以有效降低物理和网络安全事件发生的概率，减少事件导致的破坏影响。充分理解这个道理，对于网络安全应急部门完善应急响应预案和提高应急能力来说是至关重要的。相关部门在明确了网络响应与传统物理破坏响应活动之间的固有区别以后，还应该考虑物理破坏和网络安全攻击的关联关系，进而制定整体的应急响应预案。

(3) 可靠应急通信工具的重要性

可靠应急通信工具对于安全应急响应来说是非常重要的。然而，本次演习发现许多参与者缺乏使用应急通信工具的基本知识。为了最大程度地发挥这些

工具的作用,网络安全应急响应社区应该着力检查这些应急通信工具的安装部署和使用情况,对使用者加强指导和培训。

(4) 角色和责任的说明

自“网络风暴Ⅰ”以来,跨机构高级领导层面的网络事件响应协调能力已经获得了实质性的改进。继续阐明和细化角色、责任和沟通渠道,将有利于进一步提高不同组织应对网络安全事件的能力。然而,本次演习发现,行业协调委员会(Sector Coordinating Councils,SCC)、信息共享和分析中心、US-CERT、国家网络响应协调小组和危机行动小组(Crisis Action Team, CAT)的关系和责任仍需继续明确。

此外,面对物理灾害,在高级领导人之间的沟通交流通常会顺利地进行。但在网络事件中,由于网络概念的缺乏、网络术语的使用模糊,这种交流往往会陷入困境。所以,应急响应和关键基础设施保护的国家级政策和实施流程需要关于网络事件的解释说明。

(5) 非应急响应期间的信息沟通交流的重要性

在网络安全应急响应社区内,经常开展一些与应急响应无关的沟通交流也能够改进通信方式和途径,增强不同组织间的联系,进一步深入明确组织的网络安全事件响应角色和职责。这些在非应急期间交流形式的制度化和规范化,有利于发挥不同组织在真实安全应急响应事件中的作用。本次演习中,演习参与者与其协作伙伴及对应组织建立起了更为紧密的合作关系,公共和私营部门之间的沟通和协调工作得到了显著改进。

小结:“网络风暴Ⅱ”在“网络风暴Ⅰ”的基础上,继续强化对不同参演单位之间的沟通与协作关系的演练,取得了5个显著成果。各参与国与机构较上次演习而言,在遭遇网络协同攻击时,其响应、协作、信息共享等能力有了较大的提升,但仍然暴露出许多问题,这也就给今后的网络安全应急响应工作指明了发展方向。基于这些成果,隶属于国土安全部的国家网络安全局,从作为网络应急响应社区领导者的角度出发来评估自身的工作,发现存在的不足,从而采取相关措施进行改进。

2.2.3 网络风暴Ⅲ

1. 基本情况

- 演习时间:2010.09.27—2010.10.01

- 组织单位：国土安全部国家网络安全局
- 演习目的：提升联邦、州、国际政府以及私营部门之间，应对网络空间重大攻击事件的应急响应能力。
- 参演方：12 个国家政府机构、12 个联邦部门、13 个州政府、60 家私营企业。
- 演习场所：指挥部设在华盛顿。

2. 演习目标

本次演习是隶属于国土安全部的国家网络安全通信整合中心（National Cybersecurity and Communications Integration Center，NCCIC）成立后的第一次“网络风暴”演习，是对 NCCIC 协调组织能力及国家网络事件响应计划框架等预案可行性的一次检验。因此本次演习的目的主要是检验电力、水利以及银行等国家重要部门在遭受大规模的网络攻击时 NCCIC 在各机构间所发挥的协同组织和响应能力[5]。

基于上述演习目的和当前的网络安全战略及网络运营环境状况，公共和私营部门的规划者和利益相关者为网络风暴Ⅲ确立了 4 个演习目标，主要演习目标包括：

（1）演练“国家网络事件应急响应计划”（National Cyber Incident Response Plan，NCIRP）；

（2）针对网络事件，明确国土安全部的整体职责、角色；

（3）演练跨机构间的信息共享事务；

（4）演练跨机构间的行政、技术协调事务。

3. 演习范围及场景

本次演习范围主要设定在电力、水利、银行等关键基础设施领域，与前两次演习不同的是，本次演习没有在搭建好的虚拟网络环境中进行，而是首次在真实的国际互联网环境下按照国家网络事件应急响应计划进行的。

由于可信的网络环境是依赖于域名解析系统和证书授权中心的，因此，这两者往往会成为攻击者的攻击对象。演习参与者需要演练如何针对域名解析系统和证书授权中心被攻破后所带来的一系列安全攻击。本次演习场景包括：

（1）互联网更新服务被攻陷场景，即攻击者通过攻陷信息系统和通信系统来“接管”供应商的更新服务，将恶意软件或病毒通过更新或补丁包的形式迅速扩散传播出去，以此来感染或攻击更多的设备或系统。

（2）能源管理系统（Energy Management System，EMS）被攻陷场景，即攻击者通过逻辑炸弹病毒的形式来感染能源管理系统。

（3）化学和交通运输场景，即攻击者通过攻击订单管理系统和客户服务网站来干扰化学物品的正常生产和运输。

（4）联邦政府场景，即攻击者通过分布式拒绝服务攻击来阻碍联邦政府正常网络功能，并发布虚假信息来干扰政府正常工作。

（5）国际场景，即攻击者攻击澳大利亚的金融、能源、交通运输、水利等行业的网络系统，并通过恶意软件来攻击加拿大的网站和电信企业。

（6）国防部入侵场景，即模拟一个国防部员工不遵守规定，将感染了病毒的笔记本接入国防部内部网络，从而导致国防部访问节点瘫痪的场景。

（7）公共事务场景，即随着攻击的深入，攻击者大肆对安全事件进行公众报道，进而引起民众的恐慌。

（8）州政府场景，即模拟攻击者试图中断政府服务，并尝试获取州政府敏感信息的场景。

4. 演习成果

本次演习在演习规划和执行，演习后的总结等过程中收集攻防、应急响应操作等信息，取得了5个显著成果。

（1）NCIRP检验结果

NCIRP提供了一种适用于网络安全事件响应的合理框架，但是该框架中的操作流程、组织角色和职责仍不成熟，有待于改进和完善。为了能够更好地服务于国家层面的网络安全事件应急响应，NCIRP需要考虑将标准操作流程规范、应急响应社区或组织的潜在应急操作理念及合作伙伴的操作流程等因素集成起来。

（2）不同组织间的协调合作

由于演习参与者明白了合作对于双方都是有利的，因此，与网络风暴Ⅰ和Ⅱ相比，在网络风暴Ⅲ中，公共和私营部门之间的协调合作有了较大改进。联邦政府、系统所有者和运营商之间相互理解信任，在应对重大的网络安全事件时，明确了各自的角色和职责，这些都有利促进了公共和私营部门的信息共享和协调合作。

（3）安全态势感知

为了应对重大安全事件，演习发现，相关部门必须建立、发展和推广一个共享的安全态势感知系统。从“网络风暴”Ⅰ到Ⅲ，网络安全应急响应社区在共享安全态势感知方面已经获得了显著进步。

（4）国家网络风险预警等级

国家网络风险预警等级（National Cyber Risk Alert Level，NCRAL）旨在网络安全预警、网络安全应急决策、安全事件信息共享和网络事件管理等方面为网络安全应急响应共同体给出详细的等级划分。为了提高 NCRAL 的有效性，必须进一步明确如何设计警告级别变化的阈值，风险等级变化后如何进行有效的沟通和信息传递等工作。

（5）公开的网络安全报告

政府、私营部门和公众依赖于沟通途径和工具来及时地交换信息，处理网络和系统威胁问题。沟通的内容和时效性是同等重要的。因此，在发生重大网络安全事件时，及时地向公众发布网络安全报告，不仅可以帮助不同组织之间协调合作，而且还可以有效地稳定民心。

小结：“网络风暴Ⅲ”为检验国家网络安全应急响应机构的能力提供了一个真实的网络环境。国土安全部和其他参与单位一起协同合作，制定演习目标，并根据既定目标设计了相应的演习场景。本次演习为网络安全应急响应共同体检验自身网络安全预警和应急处理等方面的能力提供了条件，在国家、州、行业和组织不同层面取得了显著成果。

2.2.4 网络风暴Ⅳ

1. 基本情况

- 演习时间：2011.11—2014.1
- 组织单位：国土安全部国家网络安全局
- 演习目的：检验美国联邦政府、州、私营部门及国际组织的网络安全事件应急响应协调，信息共享，安全态势感知和决策的能力。
- 参演方：11 个国家、14 个联邦部门、16 个州政府、24 个网络安全应急协调部门和网络中心，共计约 1250 人。
- 演习场所：指挥部设在华盛顿。

2. 演习目标

本次演习的主要目标是：

（1）参照国家网络安全事件响应计划草案，进一步演练网络安全事件处理流程，不同部门之间的交互过程，以及信息共享机制；

(2) 明确和检验国土安全部及其相关部门在网络安全事件中扮演的角色和承担的职责;

(3) 检验美国联邦政府、州、私营部门及国际组织的网络安全事件应急响应协调、信息共享、安全态势感知和决策等方面的能力[6]。

3. 演习范围及内容

在2011年11月到2014年1月期间,"网络风暴Ⅳ"系列演习组织开展了15个演习项目。这些项目包括小型研讨会、州级演练和大型演练三种。本次演习主要演练预防安全事件、保护设备和系统、消除安全攻击、响应安全事件和从安全事件中应急恢复。具体演练内容涉及三个应急响应操作,即设定安全攻击指标、确认安全攻击是否发生和修复安全问题。演习参与者首先对安全攻击事件的标志和安全警告信息进行识别判断,然后综合评估以确定安全攻击事件是否发生,最后分析应该采取哪些安全机制来响应、修复此类攻击事件所导致的安全问题。本次演习内容见表2-1。

表2-1 网络风暴Ⅳ当中的演习项目一览表

演习项目	事件	备注
国家网络事件应急响应计划(The National Cyber Incident Response Plan,NCIRP)	2011.11	大规模,基于操作的训练;分布式演习;模拟召开统一协调小组(Unified Coordination Group,UCG)的职工和专家会议
网络中心董事的研讨会	2011.12	小规模研讨会;审阅、分析之前网络演习的成果和相关网络安全应急响应标准操作流程,并制定今后的改进和发展计划
公共事务桌面演习-1	2012.1	基于NCIRP,拓展安全事件范围、改进标准操作流程的小规模研讨会
缅因州演习	2012.2	支持网络安全政策发展,为未来的网络风暴及相关演习做准备工作
国家网络协调演习	2012.2	大规模,分布式演习;建成多州联合的信息共享与分析中心(Multi-State Information Sharing & Analysis Center, MS-ISAC)
公共事务桌面演习-2	2012.3	基于NCIRP,拓展安全事件范围、改进标准操作流程的小规模研讨会

续表

演习项目	事件	备注
参议院网络安全桌面演习	2012.3	根据当前立法现状，对于针对电网的攻击进行讨论及演练
俄勒冈州演习	2012.5	支持网络安全政策发展，为未来的网络风暴及相关演习做准备工作
华盛顿州演习	2012.8	支持网络安全政策发展，为未来的网络风暴及相关演习做准备工作
爱达荷州演习	2012.10	支持网络安全政策发展，为未来的网络风暴及相关演习做准备工作
国际观察和预警网络(International Watch and Warning Network，IWWN)演习	2013.3	大规模、分布式演练及讨论；审阅 IWWN 的常规计划、安全应急响应标准操作流程、政策及权限
密苏里州演习	2013.6	支持网络安全政策发展，为未来的网络风暴及相关演习做准备工作
密西西比州演习	2013.6	支持网络安全政策发展，为未来的网络风暴及相关演习做准备工作
Evergreen 演习	2013.11	大规模、分布式演练，在地方层面观察、评价遭受网络攻击的基础设施；内部交流国家安全事件信息共享与安全问题修复方式
内华达州演习	2014.1	支持网络安全政策发展，为未来的网络风暴及相关演习做准备工作

4. 演习成果

本系列演习历时四年多，取得的主要成果如下：

(1) 创建了一个论坛，为参与国家、政府机构、国际合作伙伴和其他组织或个人提供评估网络事件响应能力的服务。

(2) 讨论并确定了一个规定，即允许网络安全检查部门对各州政府和网络中心等特定的利益相关者群体，进行深入的网络安全检查。

(3) 从当地到联邦各层面，深入分析了网络安全问题，确定了重大网络事件中的资源分配过程和联邦应急响应部门职能。

(4) 对之前很少或根本没有参与网络训练的州进行训练，提升他们的网络安全应急响应能力，帮助确定其今后改进的方向，将提升这些州的网络安全应急响应能力的任务整合到国家网络安全与通信集成中心工作规划中。

(5) 加强联邦政府有效可用资源的协调和整合，应对或减轻网络安全事件的负面影响。

(6) 将新的利益相关者整合到网络风暴演习社区中来，为其提供参加网络风暴演习的机会。在国内和国际更大范围内，为利益相关者提供培训的机会。

(7) 对网络事件进行模拟，分析响应协议与网络响应计划，分析并找到这些协议和计划在信息共享、响应流程和资源分配等方面需要改进的地方。

(8) 促进发展了国土安全部 NCCIC 和网络风暴演习利益相关者之间的长期深入合作伙伴关系。

小结："网络风暴Ⅳ"演习专门开展了小型研讨会、州级演练和大型演练等不同规模的演习，以此来检验不同演习对象的应急响应能力。本次演习也进一步明确了国土安全部和国家网络安全通信整合中心的角色和职责，再次巩固了国土安全部和其他演习参与者之间的合作关系。"网络风暴"演习是一个可持续性很强的项目。每一届演习的成果和经验教训都会为下一次演习提供指导意见。"网络风暴Ⅳ"的成果和发现就可作为"网络风暴Ⅴ"继续发展的基石。例如，在本次演习中，有 6 个州是首次参与演习，这些州在演习中学习积累的经验就为他们参加下一次演习提供了有力的支持。此外，本次演习中，联邦政府辅佐州、地方政府及联邦应急响应机构的演练，也会成为下一届的演习重点内容。

2.2.5 网络风暴Ⅴ

1. 基本情况

- 演习时间：2016.3.7—2016.3.11
- 组织单位：国土安全部国家网络安全局
- 演习目的：检验美国联邦政府、州、私营部门及国际组织的网络安全事件应急响应协调、信息共享、安全态势感知和应急决策的能力。
- 参演方：9 个内阁部门、8 个州政府、12 个国际合作伙伴，70 个私营企业和组织协调单位。这些企业单位所处行业主要集中在信息系统、通信、医疗/公共卫生和零售业商业设施等关键基础设施行业。演习参与者共计约 1200 多人。
- 演习场所：指挥部设在华盛顿。

2. 演习目标

本次演习的目的是，针对关键基础设施的跨行业协同网络攻击，通过演练应急响应政策、操作流程等来加强网络安全事件的防范和应对能力。具体演习目标包括：

（1）持续地改进和完善网络安全事件应急响应协调机制，安全事件信息和安全态势共享机制，安全事件应急决策流程；

（2）评估、找出影响网络安全事件应急响应资源优化分配的相关政策、法规等因素；

（3）为演习参与者提供一个用于演练、评估和改进应急响应流程和信息共享机制的交流论坛；

（4）分析、评定国土安全部及其他政府部门在网络安全事件中所应扮演的角色和职责[7]。

3. 演习范围

演习中的攻击方利用互联网常用协议和服务的安全漏洞来发起网络攻击。演习中攻击的目标协议和服务包括：网络路由协议，域名解析协议，公钥基础设施服务。攻击目标系统涉及企业和政府系统、医疗设备和支付系统。

4. 演习成果

基于演习参与者的反馈信息和演习计划制定组在计划制定、执行及事后分析过程中记录的信息，本次演习取得了 4 个成果。

（1）国家网络事件响应计划有待完善

虽然演习参与者可以按照国际和国内制定的政策和流程，协调合作机制来进行应急响应演练，但是演习者仍需要进一步完善国家网络事件响应计划框架。例如，演习者缺少一种用于在国家层面来指导演习者进行网络安全应急响应的框架。演习者们尤其缺乏一种在大规模安全事件发生时的快速应急决策和修复的策略。此外，在本次演习中，演习管理者发现安全事件信息和安全报告中缺少对安全攻击影响评估的描述。即当演习者提供安全报告时，他们并没有对安全影响进行量化评估，所以很难对安全事件影响有较为清晰的理解。

（2）安全事件信息及时共享机制仍面临挑战

在“网络风暴Ⅴ”中，演习参与者发现安全事件信息共享的延迟也会影响安全态势感知。在演习中，大多数组织都要等安全事件信息被完全证实以后才会

发布出去。这在一定程度上延缓了安全事件信息的共享速度。在某些情况下，即使一些信息的真实有效性不能得到完全确认，这种信息在一定程度上也是可以为相关人员提供一些有用信息的。此时，发布这种信息的组织只要注意标明此类信息是未经完全验证的即可。

在演习中，许多演习参与者表示他们对于如何区分哪些信息是应该与他人共享的，以及如何设定与他人信息共享的程度等问题缺乏一个明确的理解。这也就导致演习参与者往往更愿意在其结构内部分享安全事件信息，而不愿意过多地与外界进行交流沟通。因此，这在一定程度上阻碍了信息的流通和传播速度。此外，在缺少有效信息沟通的情况下，不同组织分别采取独立的处理措施来应对安全威胁和攻击，这势必会导致安全事件信息不对称或安全应急响应步调不一致的后果。

（3）NCCIC 在信息共享过程中的重要性更加突出

本次演习证明了 NCCIC 正在逐步向国土安全部和 US-CERT 看齐，在安全事件信息和安全态势共享方面的角色越来越重要。NCCIC 和国土安全部也在努力承担安全信息和态势共享的责任，并改进相关操作流程。

（4）医疗/公共卫生和零售行业首次参演成果

第一次参加“网络风暴”演习的医疗/公共卫生和零售行业的参与者，发现了不同行业之间开展安全事件信息共享的重要性。演习还发现，这两个行业可以与其他在网络安全应急响应方面处于领先地位的能源、交通等行业合作，以此来更好地提升自身的网络安全应急能力和信息共享能力。

小结：“网络风暴Ⅴ”演习提供了一个演练国家网络安全应急响应能力的平台。国土安全部和其他参演单位一起紧密合作，根据设定的演习目标来设计具体演习场景。这些演习场景拟定了国际级规模的网络安全事件。本次演习在国家、州、行业和组织等不同层面，都检验了相关单位的网络安全预案，发现了安全问题，提高了应急响应能力，取得了显著的演习成果。

2.3　工业控制系统网络应急响应小组

如图 2-2 所示，隶属于国土安全部的国家保护与计划司的网络安全与通信办公室（Office of Cybersecurity & Communications）拥有应急通信办公室（Office of Emergency Communications，OEC）、利益相关者参与和网络基础设施可恢复部门（Stakeholder Engagement and Cyber Infrastructure Resilience，

SECIR)、国家网络安全和通信整合中心(National Cybersecurity and Communications Integration Center, NCCIC)、联邦网络可恢复(Federal Network Resilience, FNR)部门和网络安全部署(Network Security Deployment, NSD)部门。

NCCIC 包括 NCCIC 运营和集成中心(NCCIC Operations & Integration, NO&I)、美国电脑警备小组(United States Computer Emergency Readiness Team, US-CERT)、工业控制系统网络应急响应小组(Industrial Control Systems Cybersecurity Emergency Response Team)和国家通信协调中心(National Coordinating Center for Communications, NCC)四个分支。其中 ICS-CERT 是 NCCIC 的一个专门用于工业控制系统网络应急响应的重要组成部分。ICS-CERT 协调联邦、州、地方、部落和特区政府的合作关系,提高国家整体网络安全应急响应能力。ICS-CERT 与 NO&I、US-CERT、NCC 及其他国际和私营部门的网络应急响应小组(CERTs)一起合作,积极分享工控系统相关安全事件和应对措施,以此来降低关键基础设施的网络安全风险。

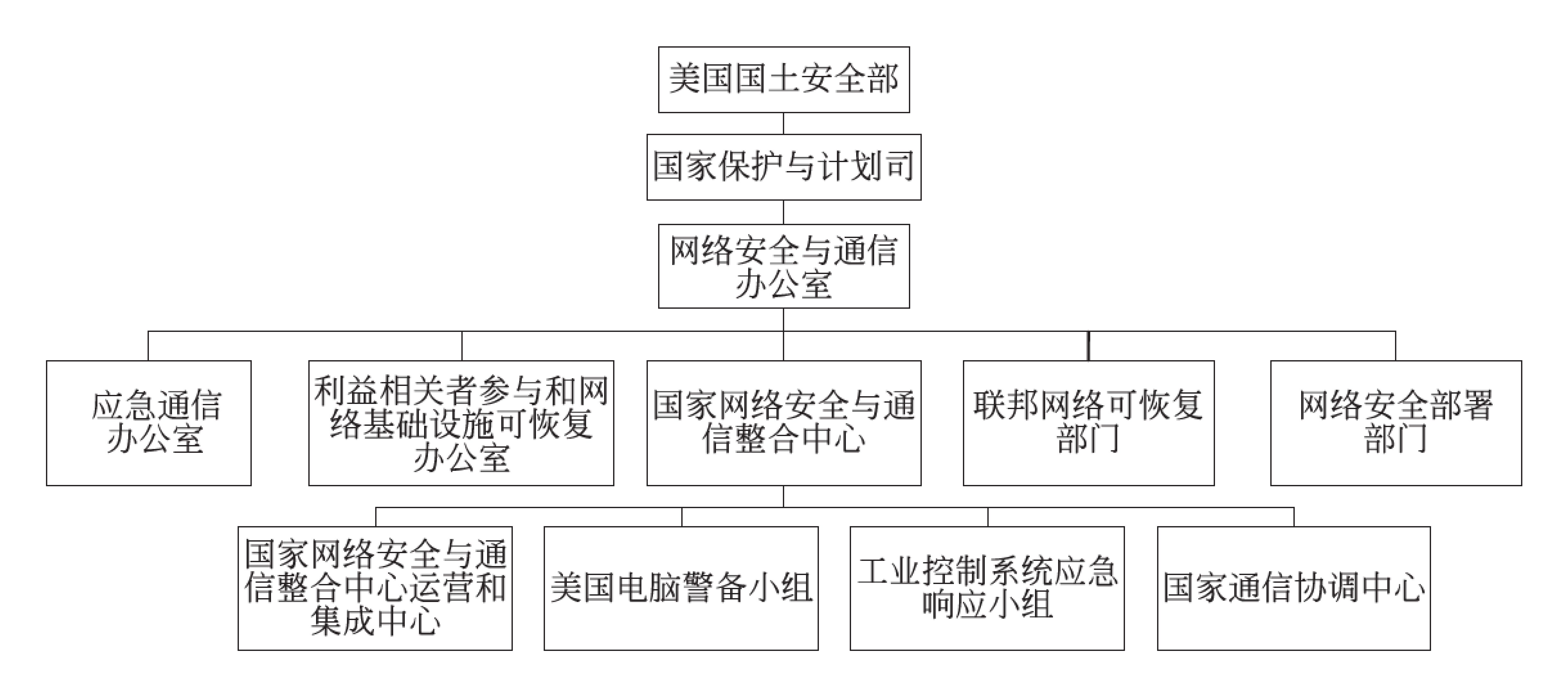


图 2-2　工业控制系统应急响应小组在国土安全部隶属关系图

2.3.1　主要职责

ICS-CERT 的主要职责分为三类:

(1) 通过分析、响应控制系统安全事件,提高政府和工业界对国家关键基础设施控制系统的安全态势感知能力,并不断提供信息安全培训,帮助这些单位更好地理解工控系统的安全风险;

(2) 协调联邦、州、地方政府,情报机构,控制系统厂商、拥有者和操作者、国

际网络应急响应小组等组织之间的控制系统网络安全事件信息共享工作，促进组织之间对安全事件信息的沟通与交流，提高现场安全事件的响应能力；

（3）通过分析控制系统脆弱性、识别恶意软件、检查验证和潜在风险分析、漏洞报告分析和发布以及对工控系统的检查评估工作来帮助控制系统厂商和拥有者/运营者发现系统脆弱性和高危的漏洞和风险并以此制定控制系统安全策略，研发安全解决方案。以下是对这三类职责的详细阐述。

1. 提高国家网络安全态势感知能力

ICS-CERT 作为国土安全部制定控制系统安全策略的重要参与单位，为了实现有效的控制系统安全风险管理，提高国家控制系统网络安全态势感知能力，ICS-CERT 致力于以下工作：

（1）分析和响应与控制系统相关的网络安全事件；

（2）分析系统脆弱性、恶意软件和数字媒介；

（3）提供在线网络安全事件响应服务；

（4）提供可直接为安全防御提供可操作指令的技术层面和战略层面的情报；

（5）报道控制系统脆弱性问题，提供相应的安全解决方案；

（6）基于信息安全产品和安全预警信息，共享和协调系统脆弱性和安全威胁信息。

ICS-CERT 在实现国土安全部所制定的控制系统安全策略中，关于参与者范围、信息共享方式、创建安全联盟等方面，形成了一个共同愿景。此外 ICS-CERT 还努力增进工业控制系统的利益相关者与政府和私营企业之间的协同合作关系，提高网络安全态势感知能力，降低关键基础设施所有行业的网络安全风险。

2. 现场安全事件响应

当收到用户的网络安全事件通知后，ICS-CERT 就会马上实施通过先进分析实验室（Advanced Analytical Laboratory，AAL）提供的恶意软件、登录文件、硬盘等分析功能进行网络安全诊断，以此来决定安全攻击所带来的危害。对于那些需要对网络攻击进行及时分析和消除的控制系统用户，ICS-CERT 可以为其免费提供现场安全事件响应服务。ICS-CERT 可以检查受攻击的控制系统网络拓扑，筛查出受感染的设备，收集必要的数据来帮助分析网络攻击，提供攻击消除策略和网络、系统安全防护建议。

3. 系统脆弱性问题处理

开展系统安全防范的首要工作就是要及时找到并消除系统潜在的脆弱性问题，以此来降低那些针对国家关键基础设施的网络攻击成功实施的概率。在处理系统脆弱性问题中，ICS-CERT 与联邦、州、地方、部落政府等公共部门，工业控制系统拥有者、运营者和厂商等私营部门一起合作，通过检测系统和收集信息、分析问题、协调制定脆弱性消除措施、应用脆弱性消除措施，信息报道 5 个步骤来应对系统脆弱性问题。在最后的信息报道环节中，ICS-CERT 会通过发布安全漏洞报告和安全建议的形式来将系统脆弱性问题通知给控制系统的用户。ICS-CERT 通过邮件和电话的形式征集控制系统安全漏洞和脆弱性问题，目前已形成了 800 多份安全漏洞警告报告和安全建议报告。此外，近几年，除了在平时不定期地发布与工业控制系统相关的安全事件、漏洞报告及安全建议以外，每年都会定期发布一份当年的网络安全报告，统计汇总分析每年的安全事件发展动态和趋势。

2.3.2　2009 年度网络安全报告

2009 年 10 月，ICS-CERT 发布了《利用纵深防御策略加强工业控制系统》网络安全报告[8]。本报告指出，工业控制系统是关键基础设施不可或缺的核心系统。日益严峻的网络安全问题及其对工业控制系统的影响已经给关键基础设施造成了重大安全威胁。为了解决工业控制系统的网络安全问题，相关人员需要对系统面临的网络安全挑战有一个清晰的认识，并掌握对应的防护措施。本报告主要介绍了目前主流工业控制系统架构，工业控制系统面临的安全挑战问题，纵深防御框架，安全防护措施等内容。其中，针对工业控制系统面临的安全威胁，本报告提出了一种纵深防御防护框架，以此来增强系统抵抗网络攻击的能力。

1. 目前主流工业控制系统架构

图 2-3 给出了企业网和控制网隔离的传统架构。企业网(Corporate LAN)和控制网(Control system LAN)物理隔离，企业网与互联网之间通过 VPN 连接，并设置防火墙进行防护。

随着控制系统的发展，通信协议逐渐网络化，网络架构逐渐开放化，因此，目前主流的工业控制系统架构发展成了如图 2-4 所示的企业网和控制网融合架构。控制网不仅与企业网之间有网络连接，而且还可以直接访问厂商网站和互联网。

图 2-3 企业网和控制网隔离的传统架构(来源:文献[8] Figure 1)

图 2-4 企业网和控制网融合的主流架构(来源:文献[8] Figure 2)

2. 工控系统安全问题

随着控制网和企业网等网络的互联互通，工业控制系统面临着一系列网络安全威胁和系统脆弱性等问题。例如：

- 在网络边界预留的后门；
- 设备或通信协议缺乏安全防护措施；
- 通用协议存在脆弱性；
- 针对现场控制设备发起的攻击；
- 数据库攻击；
- 对网络通信发起的窃听攻击和中间人攻击；
- 软件和固件存在的不兼容性问题，打补丁修复操作不恰当；
- 不安全的编码技术；
- 内部和外部人员存在不恰当的网络安全操作；
- 缺乏专门适用于控制系统的网络安全技术。

理解这些系统和网络存在的脆弱性问题及相关的攻击向量，对于建立有效的安全应对策略来说是至关重要的。

3. 纵深防御框架

本报告提出的纵深防御框架主要包括网络纵深防御策略、系统脆弱性分层防御框架、安全分区、防火墙、隔离区和入侵检测等因素。

（1）网络纵深防御策略

从纵深防御的技术角度看，网络安全除了部署专用技术来抵制特定风险以外，还需要整合公司的所有资源进行整体考虑，在不同层面上提供一个有效的完整保护。图 2-5 展示了网络纵深防御策略关键元素的总体视图。该框架包含 6

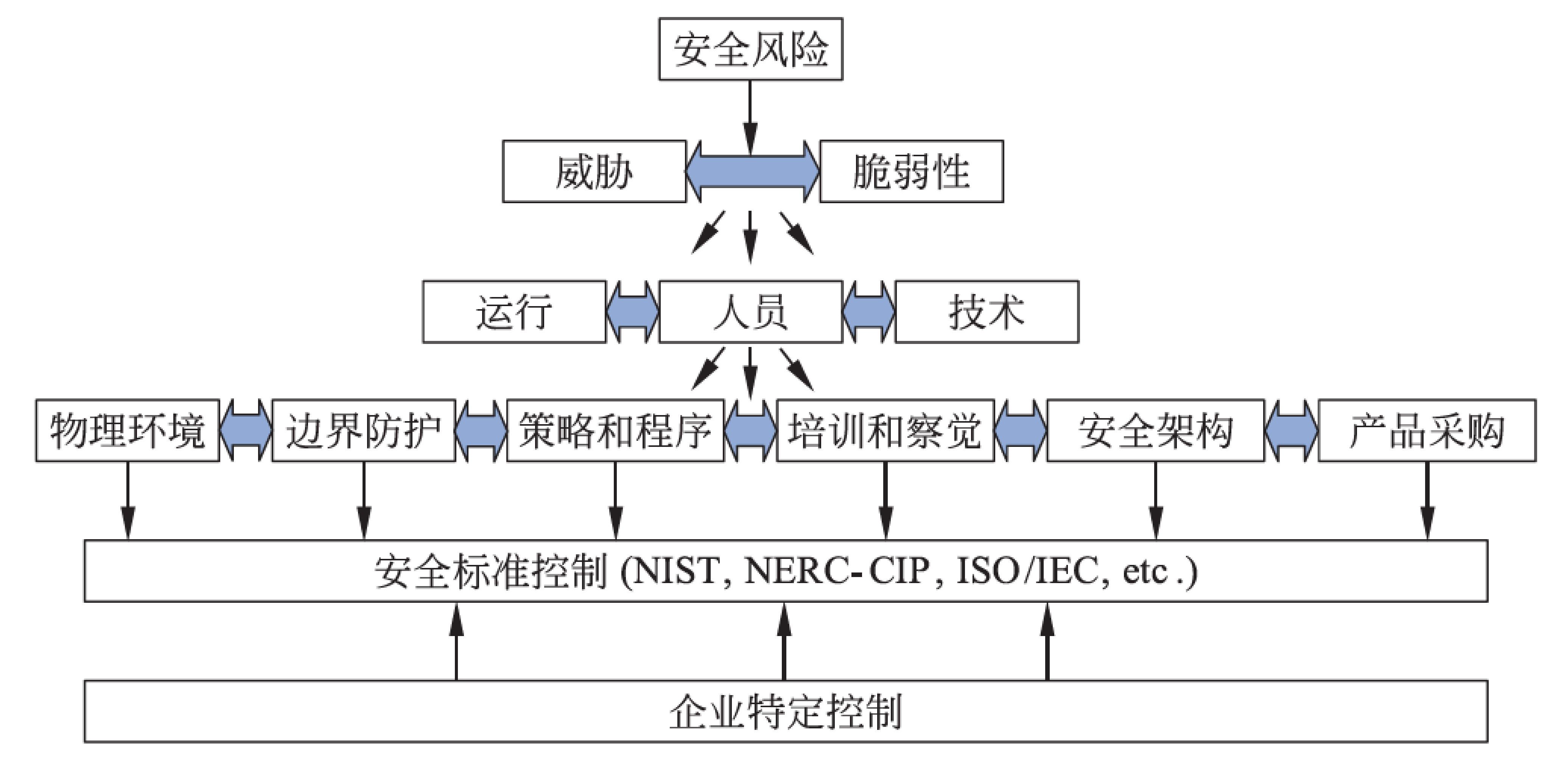


图 2-5　网络纵深防御策略

个基本原则：了解组织面临的安全风险；定性和定量地分析风险；使用关键安全资源来降低安全风险；定义每个资源的核心竞争力并识别重复区域；遵守现有的或者新出现的安全工业控制标准；定制满足工业控制系统特殊需求的防御机制。

（2）系统脆弱性分层防御框架

如前所述，工业控制系统网络目前面临的攻击包括：外围网络安全缺陷、基于通用协议的攻击、通过现场设备发起的攻击、数据库及 SQL 注入攻击、中间人攻击、漏洞修补不及时、编码方法不安全、网络安全操作流程不规范、控制系统缺乏专用安全技术。针对这些网络攻击，ICS-CSRT 从运营层面、网络层面、主机层面以及安全风险方面给出了系统分层防御框架[8]，如图 2-6 所示。

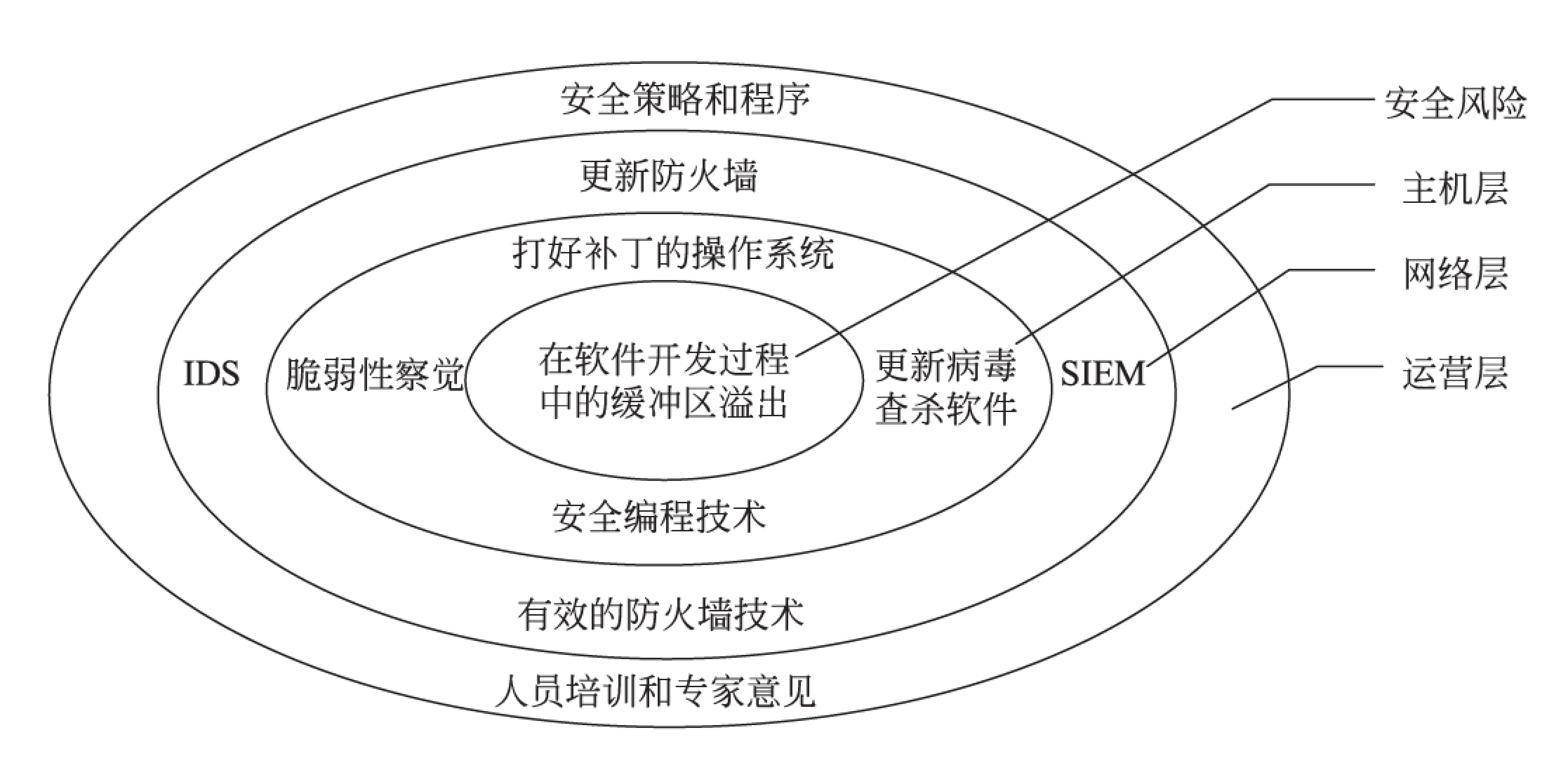


图 2-6 系统脆弱性分层防御框架（例如缓冲区溢出漏洞）

（3）安全分区

进行安全分区主要是指利用单一/多宿/双宿/级联防火墙、带有访问控制列表的路由器、可配置的交换机、静态路由、路由表和专用通信媒介等方式来对整个网络进行切分，分成不同安全等级的区域。

清晰理解如何融合所有安全技术，明确所有互联互通网络的边界，对于创建分层防御系统架构来说是至关重要的。创建安全区有助于网络管理者对网络创建清晰的边界划分，进而促进网络管理者分层次实施安全防御措施。将常见控制系统网络架构进行安全分区可以有效帮助组织创建清晰的网络边界，进而针对不同区域的网络安全威胁，运用运营、网络、主机和安全风险不同层面的技术来进行防御。如图 2-7 所示，在常见工业控制系统中，安全区域可以划分为外部域、企业域、生产/数据域、设备域、安全域。

外部域（external zone）是指不可信区域，通常是指外连到互联网、远程操作

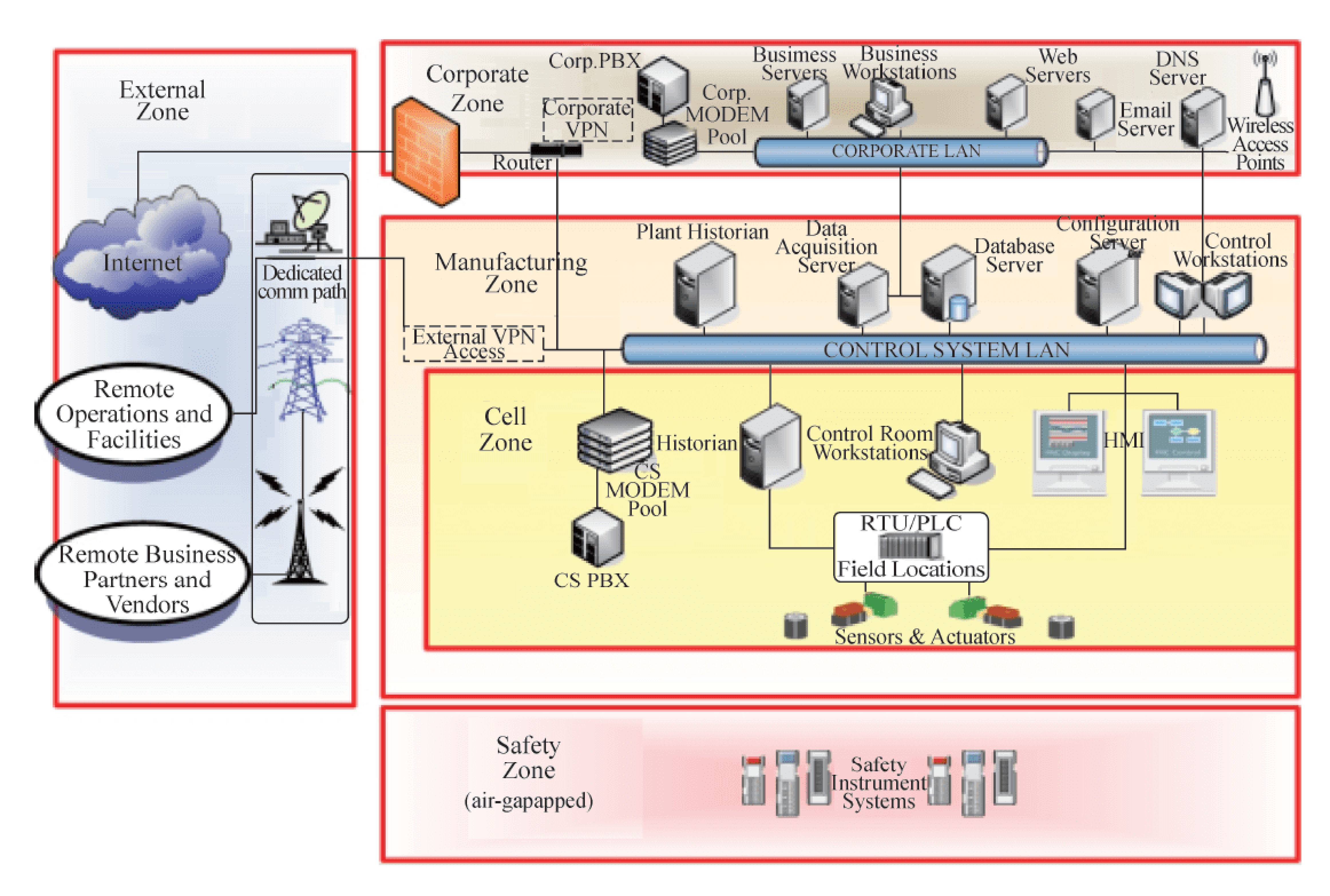


图 2-7　通用安全分区(来源：文献[8] Figure 7)

设施或设备提供商网络。在工业控制系统中,外部域风险最高,优先级最低。

企业域(corporate zone)是指企业网络通信区域,包括 IT 业务设备和系统、邮件和 DNS 等网络服务器等关键通信资源。由于企业域与外部域连接,因此企业域也将面临多种安全风险,但是由于目前企业网络安全防护机制相对成熟,企业域与外部域相比,其安全风险低于外部域,优先级高于外部域。

生产或数据域(manufacturing/data zone)是连接企业域和设备域的区域。生产域对于设备域网络和设备的持续正常运转来说是非常重要的。因此,生产域拥有较高的安全优先级。

控制域或现场域(control/cell zone)是指运行可编程逻辑控制器(Programmable Logic Controllers,PLC)、人机界面(Human Machine Interface,HMI)、执行器和传感器等工业控制设备的区域。由于设备域的功能会直接影响到控制设备的正常运转功能,所以设备域的安全优先级比生产域还要高。在现代控制网络中,设备域设备都支持 TCP/IP 或其他常见控制系统通信协议。

安全域(safety zone)中的设备由于拥有自主控制该区域内终端设备安全等级的能力,因此安全域中的设备拥有全网最高的安全优先级。

(4) 防火墙

基于图 2-7 的分区,网络管理者可以确定区域内的风险级别,进而可以选择

相应的防火墙和其他一些网络防护措施来进一步实施安全防护措施。防火墙主要包括工作于网络层的包过滤防火墙、工作于会话层的链路级网关、工作在应用层的代理网关、工作在网络会话和应用层的状态检测防火墙四种类型。图 2-8 展示了防火墙在安全分区框架中的应用位置。与图 2-7 相比,在企业域和外部域之间增加了两个企业防火墙,在企业域和数据域之间添加了两个控制系统防火墙,在控制系统局域网与外部 VPN 网络之间部署了两个控制系统防火墙,在控制域中的控制室工作站和历史数据库之间放置了现场级防火墙。

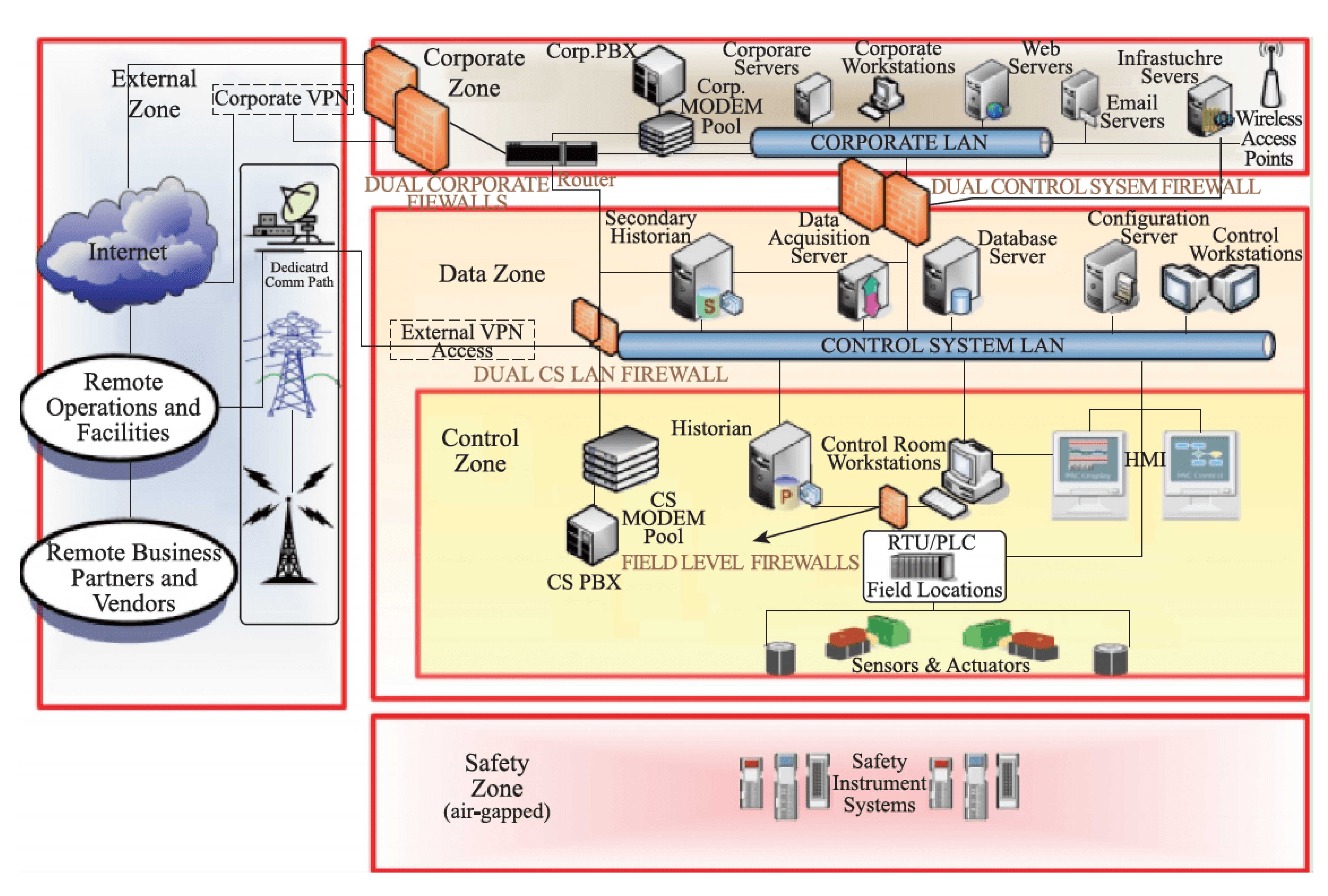


图 2-8 用防火墙来保护安全分区(来源:文献[8] Figure 8)

(5) 隔离区

当网络中部署了防火墙以后,外部网络的访问用户则不能再访问内部网络服务器了,因此,为了解决这个问题,需要在企业域与外部域之间、数据域和外部VPN 网络之间,分别建立一个非安全系统与安全系统之间的缓冲区,即隔离区(demilitarized zone, DMZ)。这些 DMZ 区一般是通过功能以及访问权限进行划分的。图 2-9 为在图 2-8 基础上添加了 DMZ 的鲁棒网络架构。使用多个DMZ 区保护信息资源是非常好的提高网络态势并将其他层纳入到深度防御策略的途径。

(6) 入侵检测系统

入侵检测系统主要包括基于主机和基于网络两种类型。在图 2-9 部署了

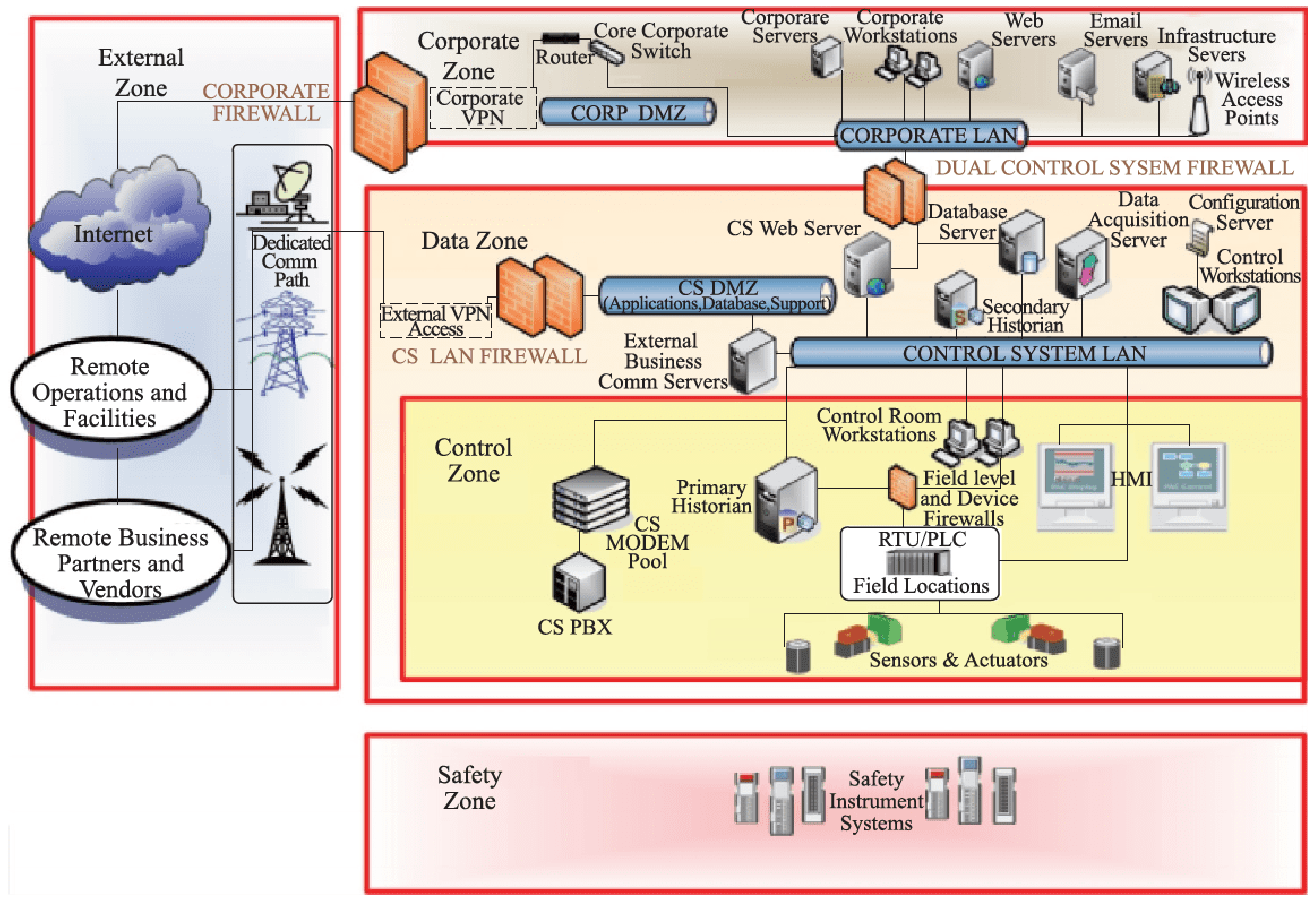


图 2-9　部署 DMZ 的框架(来源：文献[8] Figure 9)

DMZ 的框架基础上,可以通过部署基于网络的入侵检测系统,来识别网络流量、网络协议的异常行为。通过部署基于主机的入侵检测系统,来识别工控设备配置、操作与状态等方面的异常行为。图 2-10 给出了在图 2-9 基础上增加入侵检测系统之后的纵深防御完整框架。图中的"蓝色点"代表基于主机的入侵检测系统,安全事件管理系统(Security Incident Event Management,SIEM)代表基于网络的入侵检测系统。

4. 安全防护措施

工业控制系统的 5 类重要安全防护措施包括:

(1) 安全策略

应该分别在控制系统网络和主机及组件层面来制定和实施安全策略。结合系统需要的安全等级和新的安全威胁等因素,这些安全策略应该进行周期性的更新和审阅,不断得到优化和改进。

(2) 阻断对资源和服务的访问

在网络层面,通过使用防火墙或代理服务器的方式来控制对资源和服务的访问权限。在主机层面,通过使用基于主机的防火墙和杀毒软件来保护主机的

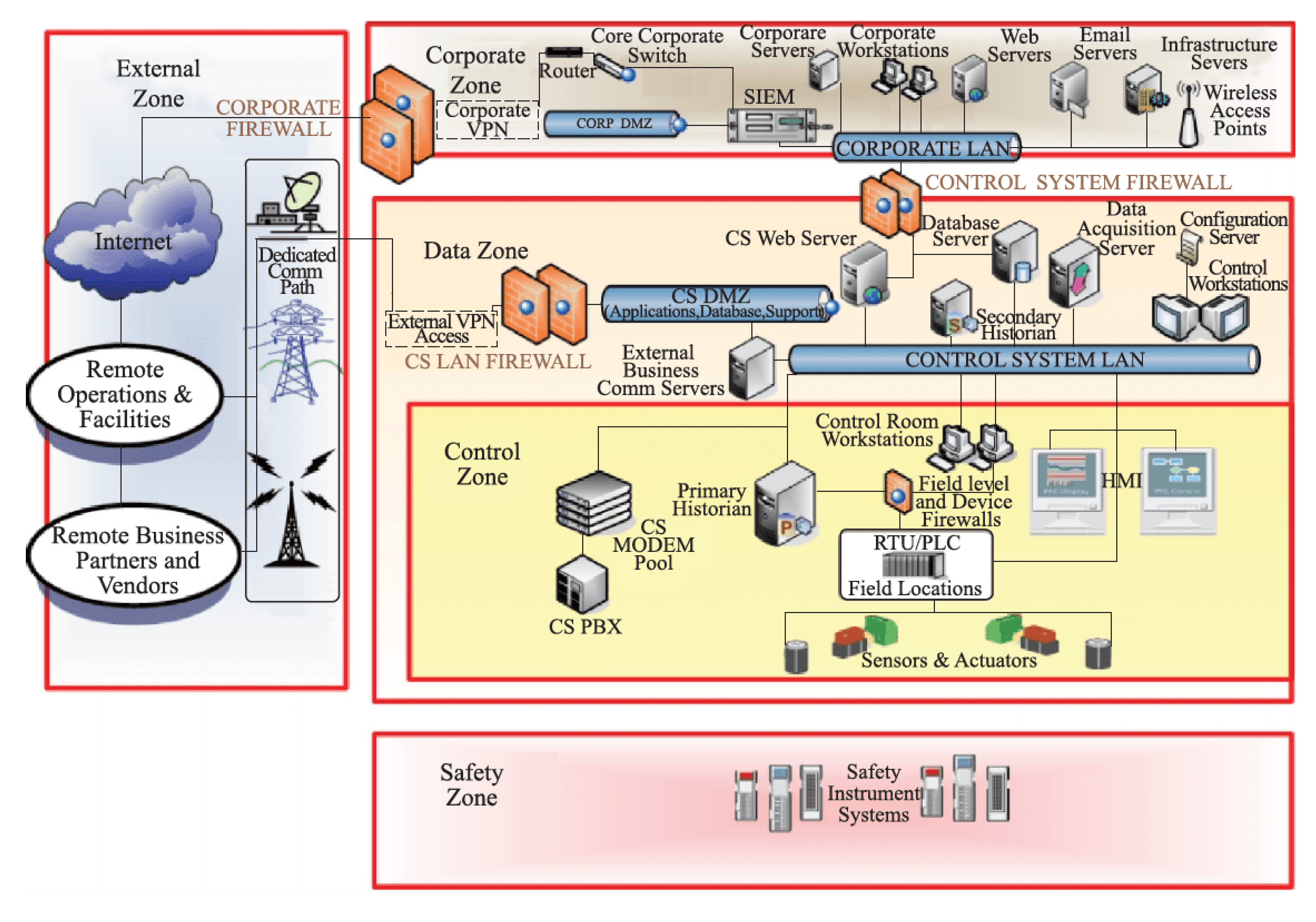


图 2-10 部署了入侵检测系统后的纵深防御完整框架图

资源和服务免遭非授权访问。

(3) 检测恶意行为

有经验的管理员可以通过定期监控分析日志文件来在网络或主机层面检测恶意行为。入侵检测系统是识别网络恶意行为的常用工具。

(4) 消除可能发生的攻击

一般情况下,某些安全漏洞是不需要处理的,因为如果修复这些安全漏洞,可能会导致系统运行效率下降或系统不可用的情况发生。此时,管理员可以通过采取一些缓解措施来控制攻击者对漏洞的利用,尽可能消除可能发生的攻击。

(5) 解决核心安全问题

安全人员或软件开发人员需要采取经常更新升级或安装漏洞补丁的方式来解决核心安全问题。这些核心问题可能存在于网络、操作系统或应用中。

2.3.3 2010 年度网络安全报告

ICS-CERT 2010 年报告[9]回顾了本年度与工业控制系统相关的震网病毒和 APT 攻击事件,分析了目前两种主要的漏洞发布方式,总结了从安全事件得到的经验教训。

1. 震网病毒(Stuxnet)

震网病毒的出现使人们开始真正关注基础设施的安全。它使人们开始深入研究现存的遗留系统中的相互依赖性和脆弱性问题。从震网病毒安全事件中我们吸取的经验和教训包括：

- 关键基础设施核心资源(Critical Infrastructure and Key Resource，CIKR)拥有者需要制定 USB 设备以及其他可移动设备在控制系统环境中的使用政策。
- 资产所有者需要采用深度防御策略、设计合理的日志监测流程、使用合适的网络监视手段来应对此类恶意软件的威胁。
- 对于公共和私营部门合作伙伴来说，及时共享威胁与分析结果信息对于开展安全防护工作来说是重中之重。

2. 高级持续性威胁攻击(Advanced Persistent Threat，APT)

由于 APT 攻击者资金充足，并且具有组织性，因此在很多情况下很难去检测、防御和彻底消除这种攻击。2010 年，ICS-CERT 和 US-CERT 帮助大量工控系统用户开展了与 APT 相关的安全检查和评估工作。此外，二者还针对如何更好地保障网络安全、检测未知恶意活动，向用户推荐了相关解决方案。从 APT 安全检查中获得的经验和教训包括：

- 资产所有者和运营者是最容易受到各种攻击的对象。
- 一个组织如果缺乏安全实践，那么就更容易遭受攻击，并且这也将使得安全检测和安全取证工作变得更难。
- 鱼叉式网络钓鱼攻击是攻击者获取攻入企业网络的切入点。
- 组织不仅需要部署更好的检测方法来检测安全威胁，更需要加强对所有控制系统网络链路的安全评估工作。

3. 漏洞发布

2010 年，ICS-CERT 及其协调中心(CERT Coordination Center，CERT/CC)，US-CERT、研究者和工业控制系统厂商一起合作及时发布相关漏洞。这种协同合作方式在研究者和厂商之间取得了非常好的效果。漏洞发布有两类方式：

- 协调发布：研究者提交漏洞给 ICS-CERT 或者厂商，延迟漏洞公布，直到厂商发布补丁。厂家并给用户留出打补丁修复漏洞的时间。

- 非预期的公布：研究者在没有通知任何协调者或者厂商的情况下公布漏洞。2010 年 ICS 的漏洞报告显示，由世界各地的独立研究者公布的非预期公布的漏洞有明显的增长趋势。

经验教训：

- 独立研究者对于提高控制系统网络安全发挥了重要作用。
- 大多数的厂商非常严肃地对待软件的安全问题，更倾向于选择协调的方式减少或最小化对用户的影响。
- 在与那些总部设立在其他国家的设备厂商之间沟通协调工业控制系统相关的漏洞时，ICS-CERT 与其他国家的 CERT 的作用同等重要。

4. USB 驱动和其他可移动介质

在震网病毒出现之前，ICS-CERT 就开始关注跟踪可移动介质感染恶意软件的发展趋势。例如职员通过将保存有恶意软件的 USB 插入到工业控制系统网络中的电脑中，就可能将病毒迅速传播到工业控制系统中。因此，资产所有者需要评估由 USB 设备和其他便携式媒介设备带来的安全风险，根据系统所有者愿意承担的安全风险等级来制定相应的安全管控策略。ICS-CERT 推荐工业控制系统拥有者和运营者阅读以下两份相关报告：

- ICS-CERT 控制系统分析报告，“针对关键基础设施的攻击向量—USB 设备驱动程序”。
- ICS-CERT 公告，“ICSA-10-238-01B—消除震网病毒”。

经验教训：工业控制系统资产拥有者需要评估使用 USB 或其他移动媒介所带来的安全风险，并制定相应的安全策略和应对措施。

2.3.4 2011 年度网络安全报告

针对工业控制系统的网络攻击行动一旦成功，就可能给诸如公共交通、电力或水利等公共服务系统带来致命的破坏，对国家政治、经济、社会及人民生命财产造成严重损失，进而危害国家安全。为了促进开展控制系统安全防护工作，国土安全部的国家网络安全局建立了控制系统安全项目(Control Systems Security Program，CSSP)。CSSP 的目标是通过协调公共部门和私营部门之间的合作关系，为工业控制系统相关利益者提供安全技术指导、安全预案和应急响应服务，来降低关键基础设施控制系统的安全风险。参与 CSSP 的成员主要包括工业控制系统利益相关者，如政府公共部门、国家实验室、企业私营部门及控制系统领域科研学者，其中典型的参与代表包括 ICS-CERT、工业控制系统联合

工作组（Industrial Control System Joint Working Group，ICSJWG）。ICS-CERT 2011 年度网络安全报告[10]回顾了 CSSP 本年度的主要工作成果。

1. CSSP 本年度工作成果总体回顾

2011 年，CSSP 为生产商、用户、经营者提供了关键基础设施安全服务，在完成以下任务的过程中，继续朝着功能安全和信息安全的方向发展。CSSP 本年度主要工作成果包括：

- 在本年度内将 ICS-CERT fly-away 安全团队部署到七个组织中，为其提供现场安全服务。
- 大约 600 人参加了 2010 年秋季和 2011 年春季的 ICSJWG 会议。
- 2011 年 8 月，CSSP 发布了网络安全评估工具（Cyber Security Evaluation Tool，CSET）4.0 版本，在 2011 年度完成了大约 1150 套 CSET 安装部署。
- 在 2011 财年完成了大约 75 次在线安全评估。
- CSSP 在国内和国际上开展了 40 多次训练课程，有超过 1300 人次参加了培训。
- CSSP 给相关的厂商提供了超过 100 份安全态势简报。

2. CSSP、ICS-CERT 本年度的主要工作成果

ICS-CERT 针对工业控制系统提供安全事件分析、响应和信息发布共享等服务，以此来消除工业控制系统的网络安全威胁和脆弱性问题。例如，ICS-CERT 针对从恶意代码感染到高级持续性威胁等一系列攻击提供在线和远程安全事件响应服务。ICS-CERT 本年度主要工作成果包括：

(1) CSET 工具

CSSP 给工业控制系统厂商和使用者提供 CSET 工具，以此来帮助他们保护国家重要网络资产。这个工具提供给使用者一种系统的和可重复实验的方法，根据公认的行业和政府标准、指南和实践来评估他们网络的安全态势。安全态势检查范围包括工业控制系统和 IT 系统。CSET 报告可以在屏幕上显示，也支持打印。报告总结了系统的安全等级，与标准对比存在的安全差距等问题。这份报告能够帮助组织制定消除安全风险的安全计划和策略。需要进行自我评估的组织可以从 CSSP 的网站上下载 CSET 软件。

(2) 网络安全培训

除了 CSET 之外，CSSP 还使用 CSET 的在线评估功能来对资产所有者进行在线培训和指导。这种培训的目的就是指导资产所有者使用 CSET 工具，以

此来更好地掌握控制系统和网络的安全态势。CSSP 提供的培训计划包括入门级、中级和高级控制系统网络课程。这些课程对于 ICS 专家和管理者是免费的。在 2011 年,CSSP 大约开展了 40 次培训课程,包括 20 多次入门级的、8 次中级和 10 次高级 ICS 课程。2011 年 4 月,CSSP 推出了管理层次的培训课程,使管理者在更高的层面上来总览控制系统网络安全态势。

(3) 厂商评估

厂商评估工作主要是针对 CSSP 分析所得到的工业控制系统环境下的设备和软件的脆弱性问题,来评估厂商的特定设备和软件的安全等级。在 2011 年,CSSP 完成了多个工业控制厂商系统的安全评估,并提出了评估结果和安全建议。ICS-CERT 将评估发现的安全问题进行通报,并为工业控制系统利益相关者群体提供识别、减少和消除安全威胁的技术指导。

(4) 安全事件信息共享

ICS-CERT 本年度向工业控制系统社区发布了 100 多次安全事件警报和安全建议。由于研究者们将 ICS-CERT 作为向工业控制系统厂商提供系统脆弱性分析结果的一个渠道,因此本年度系统脆弱性漏洞报告数目比同期增长了 600%。越来越多的工业控制系统拥有者和运营者在发生网络安全事件时向 ICS-CERT 求助技术指导和安全评估,2011 年 ICS-CERT 的网络安全事件报告也比 2010 年增长了 200%。

3. 未来工作计划

随着工业控制系统及其安全威胁的发展,未来工作需要 CSSP 和 ICS-CERT 进一步满足工业控制系统所有者、生产商和操作者的需要。给工业控制系统领域客户群体提供他们需要的安全评估工具和服务,进而保证系统安全运转,是 ICS-CERT 和 CSSP 的共同发展目标。

2012 年度的具体工作目标包括:

- 加强安全事件的应急响应能力。
- 在工业控制系统网络安全事故发生之后,为关键基础设施和核心资源所有者和运营者提供持续的现场事件响应援助,进行安全事件调查和补救。同时,ICS-CERT 和 CSSP 需要提高恶意软件的分析能力。
- 除了提供在线评估功能之外,CSSP 还将为工业控制系统安全标准研发组织提供支撑服务,并继续研发更新 CSET 工具。
- CSSP 计划修订控制系统安全策略。这个项目将会促进和维护 CSSP 网站,以此来作为控制系统网络安全信息、漏洞报告、跨部门信息共享的知

识库中心。致力于维护美国在控制系统安全领域的世界领先地位，CSSP 还会继续给 NCCIC 提供工业系统安全支持。

2.3.5　2012 年度网络安全报告

认识到控制系统对关键基础设施的重要性后，国土安全部创建了控制系统安全项目(CSSP)。该项目通过公共和私营部门合作的方式来增强控制系统网络安全，降低国家基础设施安全风险。ICS-CERT 作为 CSSP 的主要参与单位，在 2012 年继续对关键基础设施所有者、运营者、厂商、政府机构以及其他部门提供了安全产品、服务和支持。2012 年 ICS-CERT 年度网络安全报告[11] 回顾了本年度 ICS-CERT 和 CSSP 的主要工作。

1. ICS-CERT 和 CSSP 本年度的主要工作成果

2012 年，ICS-CERT 主要致力于发展国家网络安全和通信集成中心的网络安全响应能力。ICS-CERT 和 CSSP 的本年度主要工作成果包括：

- 通过安全预警和安全建议方式来提供了安全态势感知服务。
- 在恶意软件、系统漏洞等方面开展了技术分析。
- 帮助资产所有者发现、分析安全威胁，从安全事件中进行应急响应和恢复。
- 与研究者和厂商合作协调开展控制系统脆弱性监测工作。
- 2012 年，ICS-CERT 为 18 个基础设施领域的 500 个合作伙伴提供了约 60 份简报。

表 2-2 比较了在 2010 年、2011 年、2012 年中的所有的事件报告、现场事件响应、漏洞报告等方面的统计数据。其中，ICS-CERT 信息产品和漏洞报告都呈现出一个持续增长的趋势。

表 2-2　ICS-CERT 近几年活动对比表

ICS-CERT 工作指标	2010 年统计	2011 年统计	2012 年统计
ICS 事件报告	39	204	138
现场部署的 ICS 事件响应	8	7	6
ICS 相关的漏洞报告	41	141	147
ICS-CERT 信息产品	138	283	343
分发或者下载的 CSET	2394	7448	5584
现场评估	57	70	89

续表

ICS-CERT 工作指标	2010 年统计	2011 年统计	2012 年统计
专业训练	2499	1658	2241
培训课程的数量	55	47	52
ICSJWG 会员人数	N/A	1040	1416
演讲	47	164	200
会议展览	11	20	19

表 2-3 则比较了在 2010、2011、2012 财年 18 个关键基础设施领域对控制系统联盟提供的在线评估的数量。

表 2-3　分领域显示每财年的在线评估领域数量

领域	FY-10	FY-11	FY-12	累计
农业食品	0	5	0	5
银行金融	2	1	6	9
化工	0	0	4	4
商业设施	3	10	2	15
水坝	1	0	0	1
国防工业基础	1	0	12	13
应急服务	0	2	3	5
能源	13	11	7	31
市政设施	6	5	3	14
信息技术	0	3	5	8
国家纪念碑 & 图标	0	5	1	6
核反应堆材料和废弃物	0	2	8	10
邮政和航运	0	0	1	1
公共卫生和医疗	5	6	1	12
电信	0	1	0	1
交通	5	7	10	22
供水和废水系统	19	21	25	65
关键制造	2	2	1	5
总计	57	81	89	227
已评估领域的比例	11/18	14/18	15/18	N/A

表 2-3 中的最后一行比较了在当年已开展在线评估领域的数量与总的领域的数量之比。每年在线评估的总数量也呈现出一个逐年递增的趋势。

2. 下一步计划

ICS-CERT 的主要工作就是做好网络响应预案，或尽可能减低关键信息基础设施中断的可能性，以此来保护公共、经济、政府服务和国家的总体安全。ICS-CERT 会继续与公共和私营部门以及国际合作伙伴一起来准备、阻止和应对网络安全事件。ICS-CERT 提供相关资源来提高国家网络和通信基础设施的安全性、可恢复性和可靠性。为了提供综合能力，基于特定客户的需求，ICS-CERT 会继续加强网络安全响应能力。

ICS-CERT 将继续跟踪以下五个策略目标。

- 目标 1：培养公共和私营部门合作伙伴协作关系，以此来支持 ICS 的网络安全倡议。
- 目标 2：将自己打造成一个与工业控制系统安全有关的全球信息交流中心。
- 目标 3：支持强大的安全事件信息共享机制，提高事件响应能力。
- 目标 4：提高控制系统安全意识，完善利益相关者的技术知识。
- 目标 5：确保 ICS-CERT 是一个自适应和有准备的组织，有效计划、预测和管理未来的安全威胁。

2.3.6　2013 年度网络安全报告

经济和社会的安全依赖于国家关键基础设施的可靠性和可恢复性。ICS-CERT 发布的 2013 年度网络安全报告[12]介绍了如何通过建立国家级网络安全预案来提高国家网络安全态势感知和安全响应能力，保证全国关键基础设施的运行安全。

1. 国家级安全预案

对于 ICS-CERT 响应能力来说，建立国家级安全预案的关键因素包括：协作关系，统一行动，分层响应；可扩展、灵活、适应性强的业务能力。

在预防、防护、消除、响应和恢复 5 个方面，ICS-CERT 的建议如下：

- 预防——通过加强伙伴合作关系，来避免、预防、停止安全威胁或实际恐怖行为。
- 保护——通过分层保护思想，从运营层面、网络层面、主机层面以及安全

风险等方面来确保本土的关键基础设施免受恐怖袭击或网络攻击。

- 消除——形成一种可扩展、灵活和自适应的网络安全防护能力，以此来消除网络安全攻击，降低网络攻击的影响，减少生命财产损失。
- 响应——当发生网络安全事件后，通过在统一指挥下协同努力开展应急响应行动。
- 恢复——网络安全事件发生后，在进行响应的同时，开展应急恢复工作。

2. 未来计划

ICS-CERT 将会继续提高国家关键基础设施的可恢复性和可靠性，并保护其核心资源。ICS-CERT 将会与全国的关键基础设施生产供应商、运营者和资产所有者们一起合作来应对各种关键基础设施安全威胁。并且，ICS-CERT 还负责开发相关培训课程来为生产供应商、运营者和所有者提供安全技术指导。这种培训允许他们接触到全国各地更多的关键基础设施专业人员。ICS-CERT 将致力于支持关键基础设施利益相关者解决未来潜在的安全问题，继续提高网络安全响应能力。

2.3.7 2014 年度网络安全报告

ICS-CERT2014 年度网络安全报告[13]主要从安全运营和降低安全威胁两个方面总结了本年度主要工作。其中安全运营包括安全事件响应、系统脆弱性问题协调应对、安全态势感知和技术分析工作，降低安全威胁工作包括在线安全评估、网络安全评估工具 CSET 研发与推广、培训和工业控制系统联合工作组工作。

1. 2014 年主要工作成果

(1) Havex 和 BlackEnergy 安全事件响应

ICS-CERT 致力于向私营部门关键资产所有者提供关于 Havex 和 BlackEnergy 恶意软件的分类简报。这些简报内容涉及 15 个城市，时间从 2014 年 11 月 25 日到 12 月 11 日。ICS-CERT 也通过网络研讨会发布了多个警报，通报 Havex 和 BlackEnergy 恶意软件特征的详细信息及其对应的网络防御方法。

(2) Heartbleed OpenSSL 安全事件响应

漏洞协调小组及时发布了关于心脏滴血漏洞的详细报告，并邀请漏洞原始发现人员参加了两次网络研讨会。当发现心脏滴血漏洞后，漏洞协调小组立即组织应急响应行动，识别了受影响的工业控制系统产品，并及时发布了多次安全

警报。此外,小组还与工业控制系统生产厂商积极配合,防止后续发生任何重大安全事件。

(3) 在线培训

ICS-CERT 培训小组推出了具有混合学习方法的新的在线培训模块,这种模块能够更容易和更有效地访问课程教材,减少培训材料的冗余。

(4) CSET 工具更新发布

在 2014 年,CSET 开发小组发布了 CSET 的两个版本:在 2 月份发布了 6.0 版本,在 8 月份发布了 6.1 版。最新的版本包含了国家标准和技术研究院的《提高关键基础设施网络安全的框架规范》,允许资产所有者创建自己的安全问题题库,提高工业组织创建和分享安全题库方面的协作能力。

(5) 安全事件信息上报

2014 年 ICS-CERT 继续加强它与资产所有者之间的信任关系,鼓励关键基础设施所有者上报网络安全事件信息。2014 年,ICS-CERT 老客户的数量继续增长,并在观察威胁活动方面积极分享信息。如图 2-11 所示,在 2014 年的安全事件报告主体统计中,关键基础设施拥有者/运营者上报的安全事件就占到了 16%。

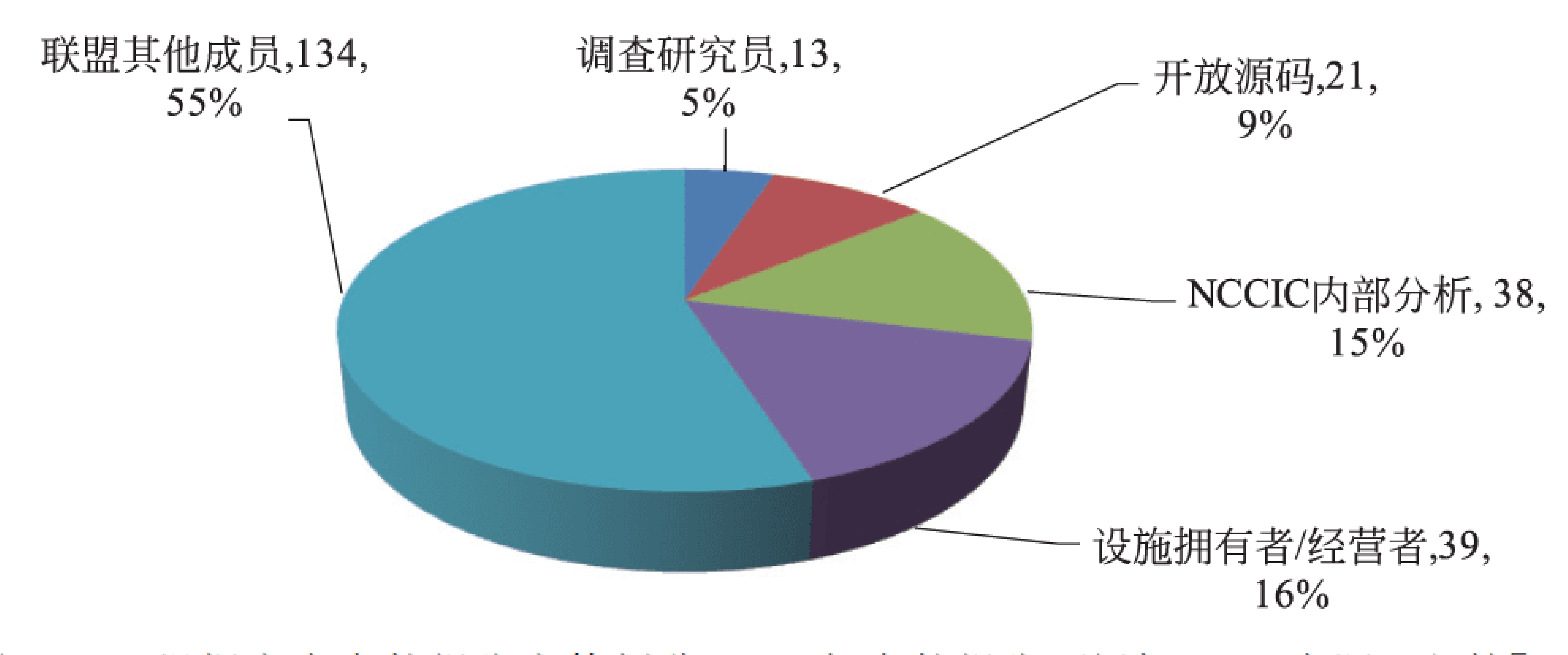


图 2-11　根据安全事件报告主体划分 2014 年事件报告(总计 245)(来源:文献[13])

(6) 安全事件攻击分析

在 2014 年,ICS-CERT 接收并响应了由设施所有者和业界合作伙伴上报的 245 件安全事件。如图 2-12 所示,在 2014 年发生网络安全事件的行业分布中,能源行业位居第一位,其次是关键制造业。对于攻击方法或途径,包括但不限于以下方面:对于 ICS/SCADA 网络的非授权访问和开发;网络扫描和探测;可移动介质;暴力破解入侵;不健全的认证机制;有针对性的鱼叉式网络钓鱼活动;SQL 注入;水坑攻击;社会工程学。图 2-13 显示了根据攻击类型划分的 2014 年安全事件统计情况。

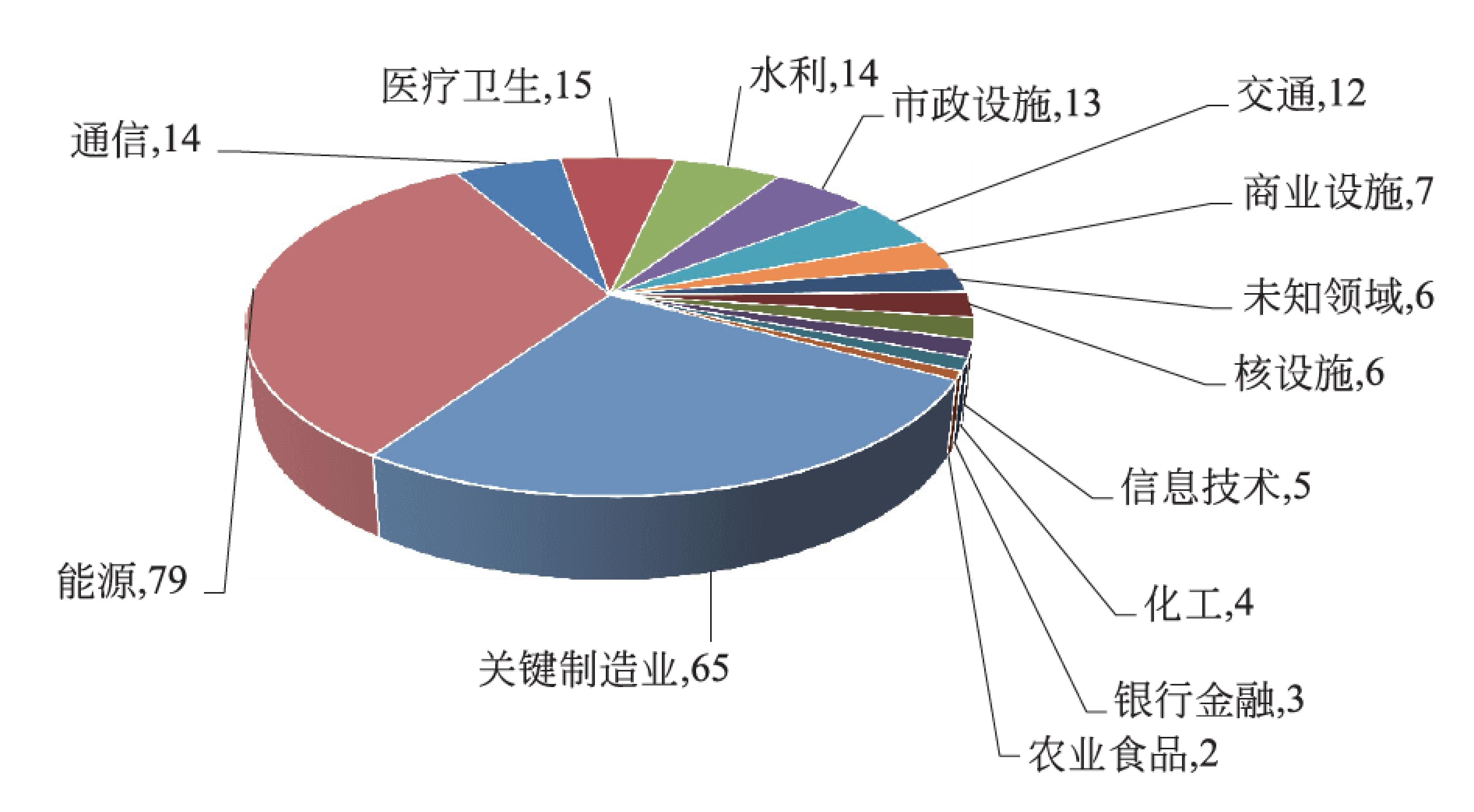


图 2-12　根据安全事件发生行业划分 2014 年事件报告(总计 245)(来源：文献[13])

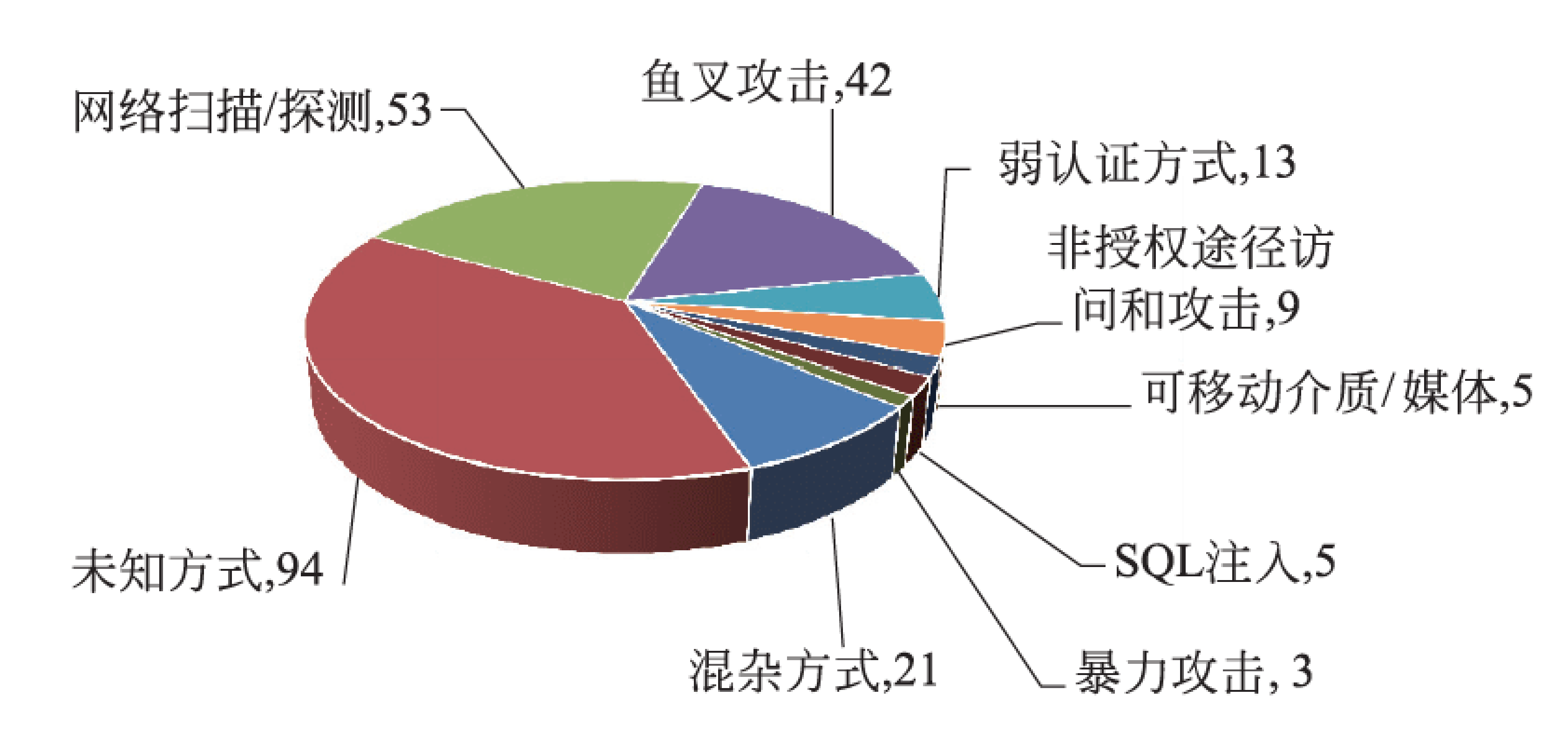


图 2-13　根据攻击类型划分 2014 年事件报告(总计 245)(来源：文献[13])

在 2014 年,因为鱼叉式攻击效果明显,技术成熟,所以鱼叉式攻击仍然是本年度最流行的一种攻击手段。水坑攻击作为一种新的技术被用于在各种生产商的网站上安装特洛伊木马软件,用户软件更新时,在毫无防备的用户网络中安装恶意软件。许多被侵入的用户甚至都没有意识到他们已经受害了。社会工程学也是最常用的手段,并且增加了对可移动媒介的使用。此外,本年度还发现了多个针对工业控制系统特定功能多个系列的恶意软件。为了应对这些安全威胁,ICS-CERT 提供了远程在线的事件响应支持,分析事件是由人为因素还是恶意软件所致。

(7) 高级分析实验室研发成果

高级分析实验室(The Advanced Analytical Laboratory,AAL)提供了研究和分析能力,能够支持 ICS-CERT 完成安全事件评估、响应和漏洞发布等行动。AAL 的网络安全研究涉及数字媒介的取证分析、工程恶意软件逆向分析以及在线或者远程的网络事件分析。2014 年,AAL 主要进行实验室分析能力的自动化和优化工作,主要在以下几个方面进行了改进:完成了远程事件响应网络

(Remote Incident Response Network,RIRN);将取证分析工具自动化并集成到一个网络分析工具(Analyst Network Tool,ANT)套装软件内;开发一个在事件响应期间分析安全事件数据关联的自定义应用程序,即广泛事件响应关联(Correlating Extensive Incident Response, CEIR)工具。

(8) 安全评估

ICS-CERT 评估部门在 21 个州进行了 104 次在线网络安全评估活动,以此来帮助关键基础设施资产所有者评估他们的工业控制系统的整体网络安全等级,提高其安全防护和应急能力。这些在线网络安全评估活动主要包括以下评估方式:现场指导网络安全分析工具(CSET)评估,设计结构审查(Design Architecture Review, DAR),网络架构检验和确认(Network Architecture Verification and Validation,NAVV)。图 2-14 显示了 2014 年 ICS-CERT 在各个州在线评估的数量。

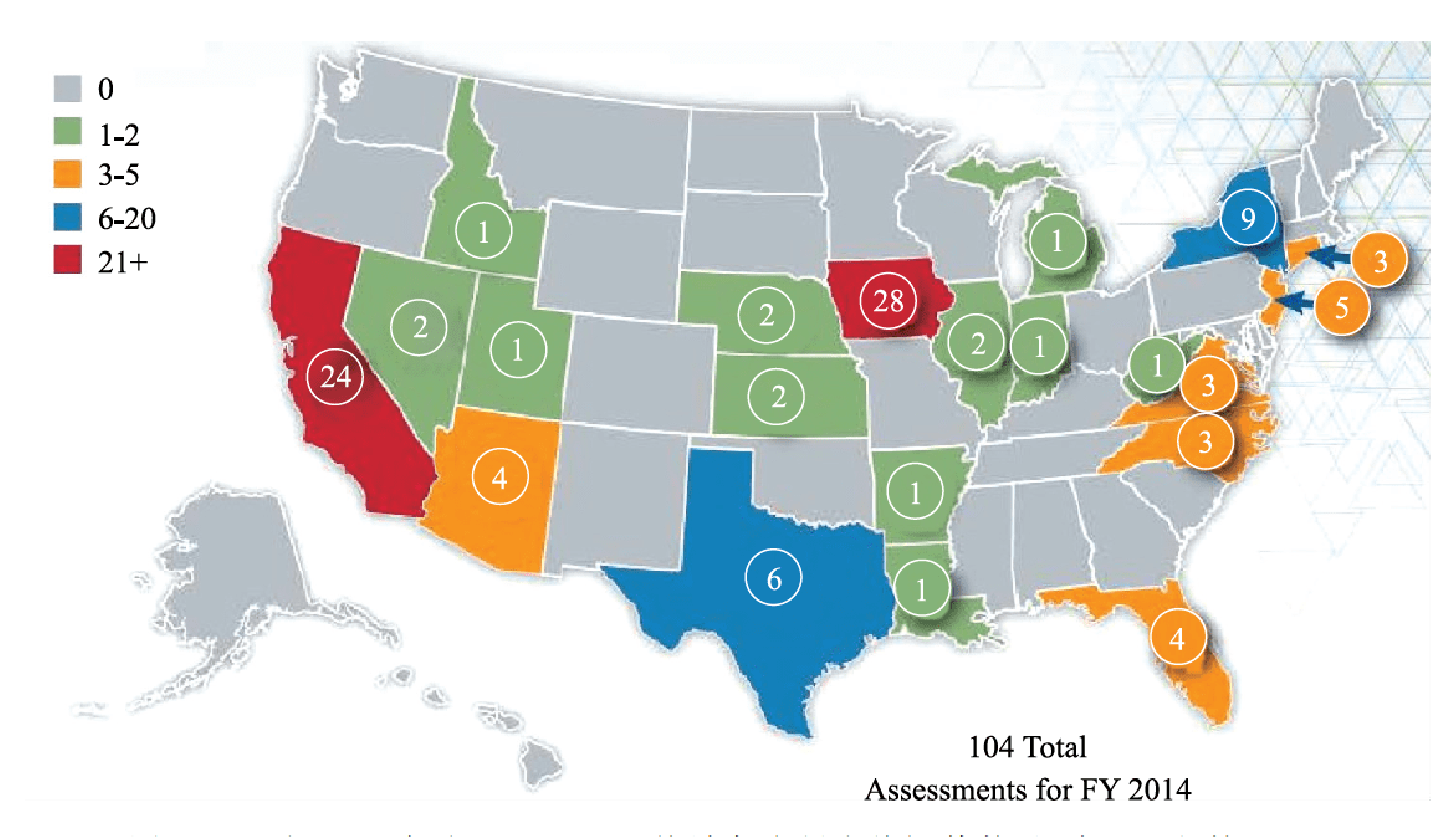


图 2-14　在 2014 年由 ICS-CERT 统计各个州在线评估数量(来源:文献[13])

表 2-4　根据评估类型划分的在线评估数量

评估类型	2014 财年数量
CSET	49
DAR	35
NAVV	18
企业基于主机的分析	2
总计	104

2. 未来计划

2015 年，ICS-CERT 将会继续提高网络安全能力，扩展支持 16 个关键基础设施领域所有工业控制系统利益相关者的安全服务。通过实时有效的态势感知、信息共享策略，ICS-CERT 将会继续与行业和政府相关参与者一起合作努力来降低关键基础设施面临的网络风险。

为了进一步提高在线评估，ICS-CERT 还将会为关键基础设施资产所有者在 CSET 使用方面进行更多的一对一服务，帮助他们找出安全问题，提高安全防范和安全响应能力。除了扩展现场评估之外，ICS-CERT 还将开发和出版有关安全建议和防御策略的控制系统专用技术指南来应对不断变化的安全威胁。2015 年的其他目标还包括改善并扩充 ICS-CERT 技术团队及工具。此外，ICS-CERT 还将继续提高培训课程质量，更好地满足关键基础设施资产拥有者技术需求。

2.3.8 2015 年度网络安全报告

ICS-CERT 与 NCCIC 一起联合发布了 2015 年度网络安全报告[14]。本报告回顾了 2015 年 NCCIC 和 ICS-CERT 取得的工作成果，并为 2016 年做好了工作计划。

1. 2015 主要工作成果

(1) 奥巴马总统视察 NCCIC

2015 年 1 月 13 日，奥巴马总统视察 NCCIC，并发表了关于新网络安全法的讲话。讲话指出，网络安全威胁已经给国家安全提出了巨大的挑战，并着重强调了建立一个公共部门和私营部门之间可靠信息共享和协同应急响应机制的重要性。

(2) ICS-CERT 获得政府信息安全领导奖社区意识奖

2015 年 5 月，由于 ICS-CERT 在 BlackEnergy 和 Havex 攻击事件中做出的突出贡献，ICS-CERT 被授予第 12 届美国政府信息安全领导奖社区意识奖。

(3) 技术培训

2015 年 8 月，ICS-CERT 培训小组更新了既有的虚拟学习门户。本次升级与联邦法律里面规定的基于云的应用一致，提升了图形用户界面，降低了运营成本。新的虚拟学习门户也促进了项目提供持续教育单元的目标。

(4) 安全评估

ICS-CERT 对 16 个关键领域的 8 个领域进行了 112 次评估，其中，38 次是使用网络安全评估工具(Cyber Security Evaluation Tool，CEST)，46 次是使用

设计结构审查(Design Architecture Review,DAR)工具,28 次是使用网络架构验证和确认(Network Architecture Verification and Validation,NAVV)工具。其中,从 2014 年 9 月—2015 年 2 月和 2015 年 11—12 月两个时间段内,ICS-CERT 总共进行了 55 次评估工作,以此来提高关键基础设施所有者、运营者和控制系统厂商(如表 2-5 所示)的网络安全态势感知能力。在这 55 次现场评估中,23 次是使用 CSET,21 次是使用 DAR,11 次是使用 NAVV(如表 2-6 所示)。

表 2-5　不同领域评估情况表

评估区域	2014 年				2015 年				总计
	9 月	10 月	11 月	12 月	1 月	2 月	11 月	12 月	
化工	—	—	—	—	—	—	—	—	—
商业设施	2	—	—	—	—	—	—	4	6
通信	—	—	—	—	—	—	—	—	—
关键制造	—	—	—	—	—	—	—	—	—
大坝		—	—	—	—	—	—	—	—
国防工业基础		—	1		1		—	—	2
应急服务	—	—	—	—	—	—	—	—	—
能源	2	1	3	2	—	4	2	—	14
金融服务	—	—	—	—	—	—	—	—	—
食品和农业	—	—	—	—	—	—	—	—	—
市政设施		—	—	—	2	—	—	—	2
医疗和公共卫生	—	—	—	—	—	—	—	—	—
信息技术	—	—	1	—	—	—	1	—	2
核反应堆材料和废弃物		—	—	—	—	—	—	—	—
运输系统	—	1	1	2	—	—	—	—	4
供水与废水系统	1	6	—	1	3	3	—	11	25
月度总计	5	8	6	5	6	7	3	15	总计 55 次

表 2-6　不同评估工具统计表

评估工具	2014 年				2015 年				总计
	9 月	10 月	11 月	12 月	1 月	2 月	11 月	12 月	
CSET	3	5	4	2	3	1	1	4	23
DAR	1	3	1	3	2	3	1	7	21
NAVV	1	—	1	—	1	3	1	4	11
月度总计	5	8	6	5	6	7	3	15	55

（5）开发 CSET 6.2 和 7.0 版本

2015 年，CSET 开发小组发布了 CSET 的两个版本，1 月份的 6.2 版和 8 月份的 7.0 版。最新版本功能包括了新的界面、新的安全标准，提升了相关功能和评估文件的加密能力。2015 财年，ICS-CERT 在 120 个国家发布了 CSET 的 7400 份拷贝版。

CSET 开发小组还在 2015 年秋季的工业控制系统联合工作组会议上介绍了 CSET 的最新变化，对 CSET 进行了演示，阐述了工具的新目标，突出显示了最新功能。本次介绍还包括 CSET 可能的新功能的调查问卷，如图 2-15 所示，调查结果明确说明了资产所有者期望在控制系用系统架构方面的安全指导。

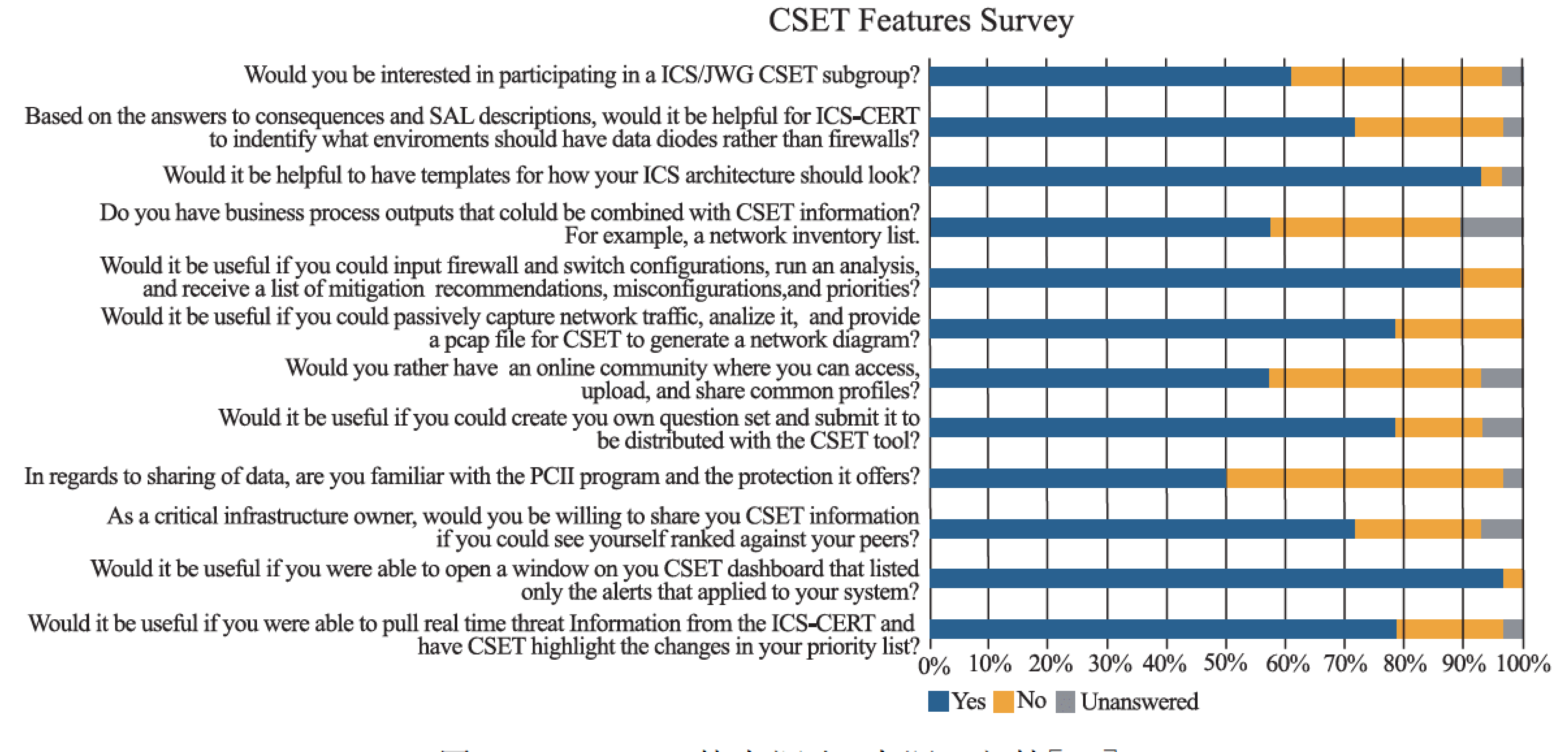


图 2-15 CSET 特点调查（来源：文献[14]）

（6）安全事件响应和安全漏洞协调处理

在 2015 财年，ICS-CERT 响应了 295 起网络安全事件。这比 2014 年增长了 20%。如图 2-16 所示，关键制造业在 2015 年发生了 97 起安全事件，成为所有行业中发生安全事件最多的行业，这主要是因为在 2015 年针对关键制造企业发生了大范围的鱼叉攻击。其次就是能源行业，发生了 46 起安全事件。然后水利和污水行业排列第三，发生了 25 起安全事件。同时，ICS-CERT 共协调处理了 321 个安全漏洞，较 2014 年的 231 件约增长了 39%。漏洞协调小组减少了漏洞处理的平均天数。

2015 财年，ICS-CERT 应急响应了大量的由于网络架构不合理所导致的安全事件，比如工业控制网络直接连接到互联网或者企业网。这是非常有利于攻击者发起鱼叉式网络钓鱼攻击的。图 2-17 显示了在 2015 财年入侵事件中使用

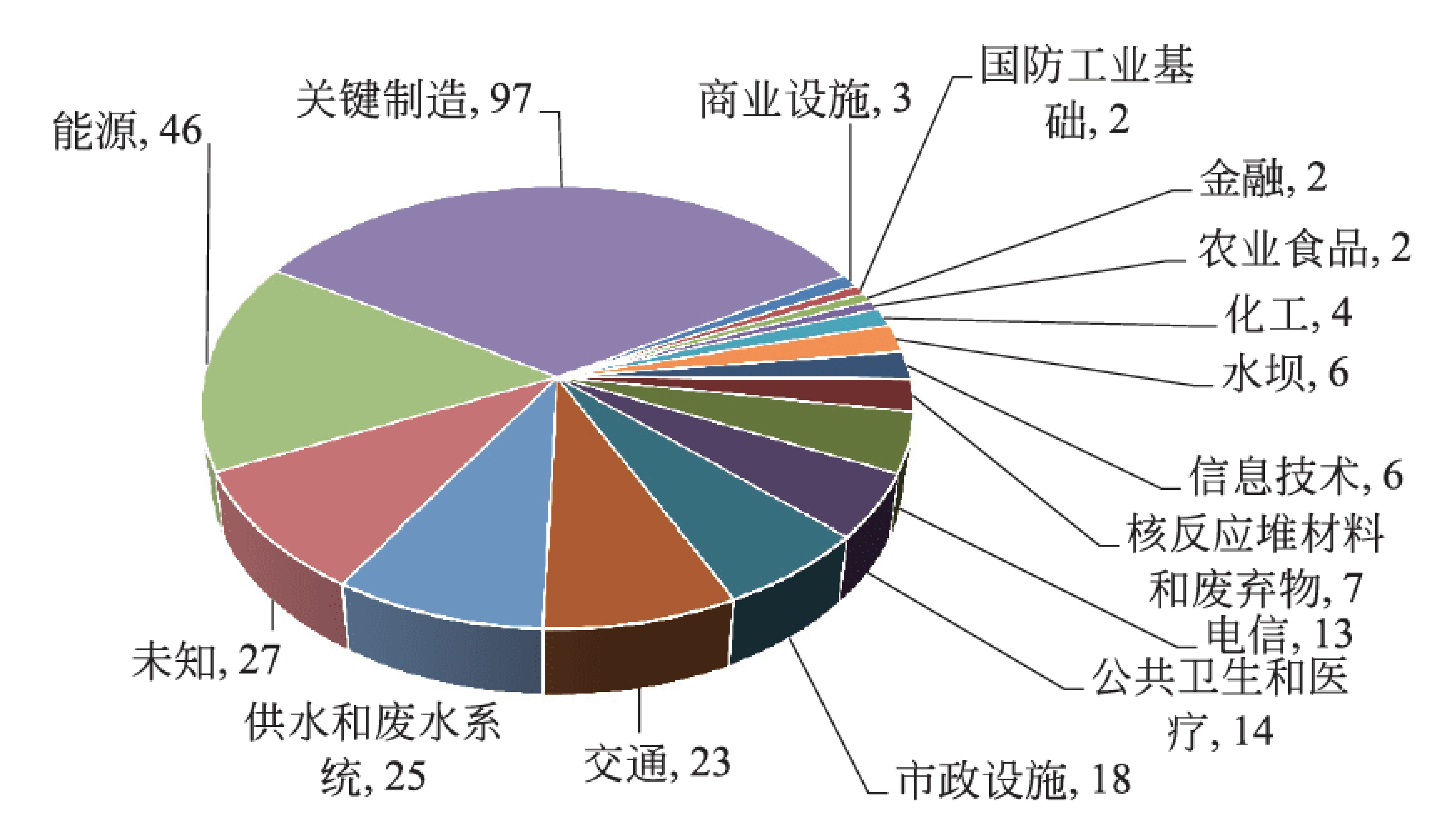


图 2-16　按区域划分的 2015 财年网络事件，共 295 件(来源：文献[14])

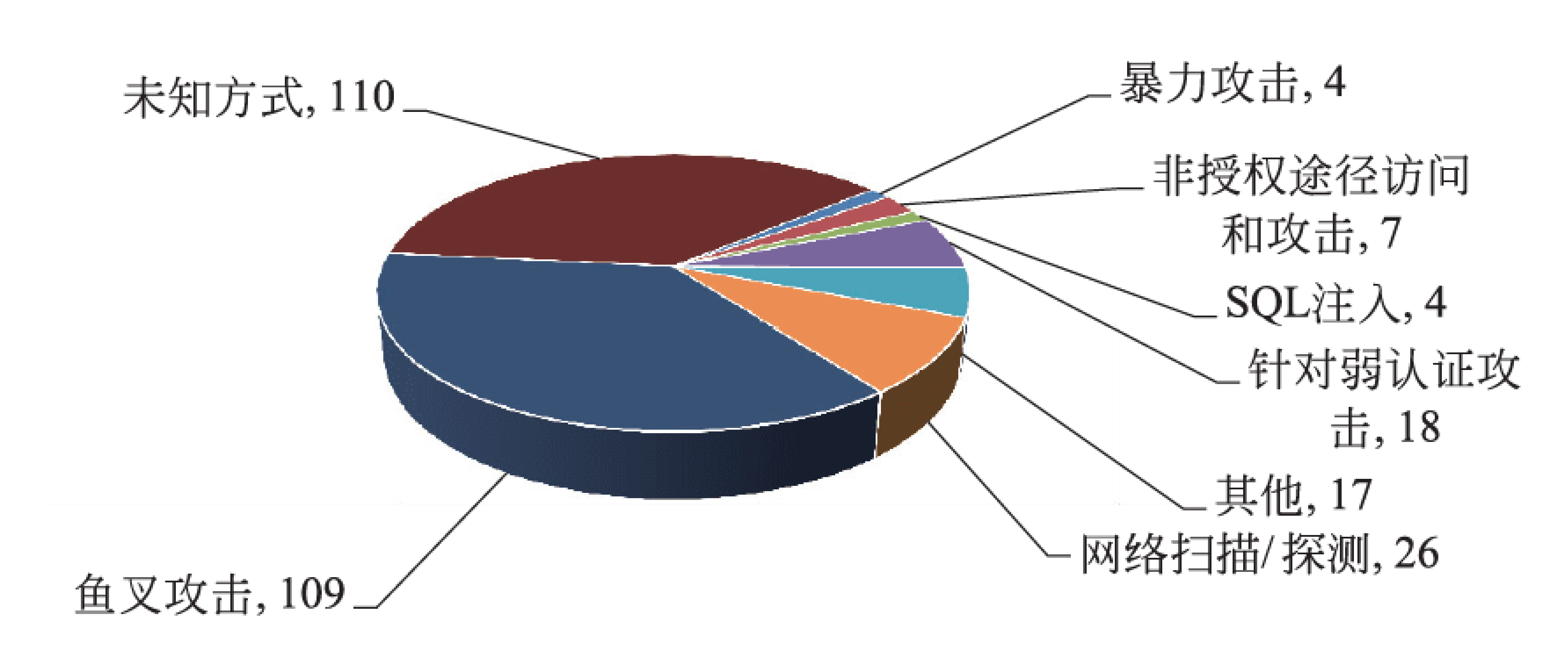


图 2-17　按试图感染途径划分的 2015 财年网络事件，共 295 件(来源：文献[14])

技术的饼状图。其中有 37%的安全事件来自于钓鱼攻击。

2. 未来计划

在 2016 年，ICS-CERT 将会继续拓展其在 16 个关键基础设施行业中的网络安全能力，为所有工业控制系统利益相关者提供更好的安全服务。ICS-CERT 也将继续与工业界和政府合作伙伴协调合作，一起通过及时有效的安全事件信息共享方式来尽可能降低网络系统的网络安全风险。为了更好地开展在线安全评估工作，ICS-CERT 也将会继续扩招人员并努力加强为关键基础设施资产所有者提供使用 DAR 和 NAVV 工具的一对一指导服务能力。此外，在 2016 年，ICS-CERT 还将为联邦政府机构提供全方位的控制系统安全评估。

2.3.9　2016 年度网络安全报告

ICS-CERT 发布的 2016 年度网络安全报告[14]总结了 2016 年 ICS-CERT 的主要工作成果，并展望了 2017 年的工作方向和目标。

1. 2016 年主要工作成果

表 2-7 给出了 2014 年至 2016 年 ICS-CERT 的主要工作对比情况。表 2-8 给出了近几年在不同领域的评估统计情况。

表 2-7 ICS-CERT 近几年活动对比表

ICS-CERT 工作指标	2014 年	2015 年	2016 年
ICS 事件报告	245	295	290
现场部署的 ICS 事件响应	4	5	3
ICS 相关的漏洞报告	159	189	187
ICS-CERT 信息产品	339	332	274
分发或者下载的 CSET	5132	7565	10 249
现场评估	104	112	130
专业训练	800	1330	1622
培训课程的数量	21	29	29
ICSJWG 会员人数	1726	1912	2476
演讲	168	342	343

(1) 安全评估

如图 2-18 所示，在 2016 年，ICS-CERT 对 19 个州的 12 个关键基础设施领

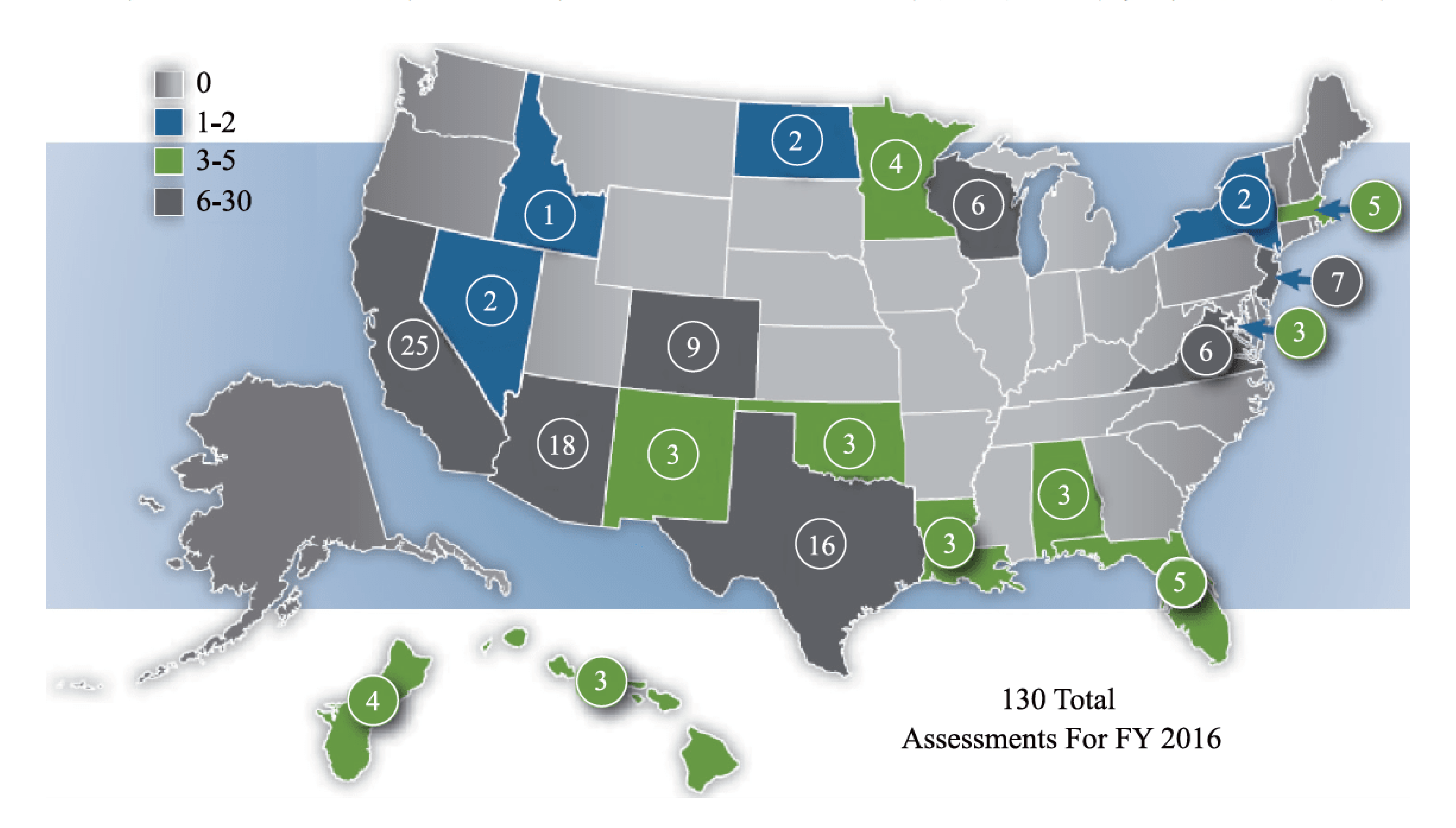


图 2-18 ICS-CERT 2016 年对 19 个州开展安全评估情况图

表 2-8 不同领域评估统计表

评估区域	2014 财年	2015 财年	2016 财年
化工	1	3	7
商业设施	2	0	4
通信	0	0	5
关键制造	0	0	5
大坝	0	0	2
国防工业基础	0	3	0
应急服务	0	10	3
能源	43	33	22
金融服务	0	0	0
食品和农业	0	0	3
市政设施	5	12	10
医疗和公共卫生	0	0	0
信息技术	0	3	3
核反应堆材料和废弃物	5	0	0
运输系统	10	9	10
供水与废水系统	38	39	56
总计	104	112	130
已评估行业	7/16	8/16	11/16

域进行了 130 次评估，其中，32 次是使用网络安全评估工具 CEST，55 次是使用设计结构审查 DAR 工具，43 次是使用网络架构验证和确认 NAVV 工具。ICS-CERT 在本年度还参与了区域弹性评估项目(Regional Resiliency Assessment Program，RRAP)。RRAP 是一个对特定区域的特定关键基础设施所开展的安全评估项目。在 2016 年，ICS-CERT 为 RRAP 提供了 16 次基础设施安全评估服务。基于这些安全评估工作，在 2016 年 8 月，ICS-CERT 安全评估小组发布了 2016 年度 NCCIC/ICS-CERT 工业控制系统安全评估总结报告。

此外，ICS-CERT 在 2016 年还参与了联邦设施控制系统安全项目(Federal Facility Control Systems Security Program，FFCSSP)。FFCSSP 是由 ICS-CERT、联邦保护服务(Federal Protective Services，FPS)、总务管理局(General Services Administration，GSA)联合开展的政府设施控制系统安全评估项目。

(2) 开发 CSET 7.1 和 8.0 版本

ICS-CERTCSET 研发团队于 2016 年的 2 月发布了 CSET 的 7.1 版本，于 9

月发布了8.0版本。最新版本的CSET实现了最新的工业控制系统协议，优化了用户操作界面。在2016年，ICS-CERT在120个国家部署安装了10 000多个CSET工具。

（3）安全事件响应

在2016财年，ICS-CERT事件响应小组完成了290起安全事件。其中，排名前三的行业包括，关键制造行业63起，通信行业62起，能源行业59起。在所有这些安全事件中，网络钓鱼是最主要的攻击方式，有26%的安全事件都是由于网络钓鱼引起的。其次则是网络扫描和嗅探，有12%的事件是由于网络扫描和嗅探发起的。

2015年12月23日，乌克兰电网系统遭黑客攻击。该事件发生后，NCCIC/ICS-CERT和联邦调查局，国土安全部及其他联邦机构一起协助乌克兰来分析、应对此次攻击。在2016年3月和4月，ICS-CERT和联邦调查局组织电网设施拥有者和相关人员开展了一系列线下和线上的研讨会，为他们提供了攻击事件分析结果信息。

（4）组织召开工业控制系统联合工作组会议

本年度，工业控制系统联合工作组成功组织召开了春季和秋季两次工业控制系统联合工作组会议，一共有594人参会。春季会议中就有306个工业控制系统利益参加，这是目前为止规模最大的一次会议。

（5）技术分析

2016年，ICS-CERT先进分析实验室对100个恶意软件样本进行了深度研究分析，向工业控制社区发布了多个网络安全警报。

（6）技术培训

在2016财年，24 350个学生注册了ICS-CERT在线培训课程，并已有17 773个学生完成了整个培训课程。ICS-CERT培训团队在匹兹堡、波士顿等地开展了多次技术培训活动，共计有1076人次参加了培训。

2. 未来工作

在2017年里，ICS-CERT将继续提高国家16种关键基础设施行业的网络安全能力。其私营部门安全评估、CSET、培训等团队分别制定了各自2017年的具体工作目标：①私营部门安全评估团队将与设施拥有者们一起来制定因地制宜的安全评估方法。团队将综合利用CSET、DAR和NAVV评估工具来为设施拥有者们提供综合的安全评估服务。②CSET研发团队计划发布两个新的版本，将实现国家标准与技术研究院NIST 800-53第四版本和北美电力可靠性公

司北美电力可靠性委员会关键基础设施防护第六版等标准内容。③培训团队将在 2017 年继续加大在攻防训练方面的培训规模，拟自春季开始每三周组织一次培训。与此同时，团队还会进一步增加在线培训课程，为用户提供额外的课程练习。

总之，在 2017 年，ICS-CERT 将会为了实现自身的职责，继续通过加强公共和私营部门合作关系，来提升控制系统安全防护能力。

2.4　网络安全部门项目

在 2011 年，为了应对不断增加的网络安全任务，国土安全部（DHS）下属高级研究计划局（Homeland Security Advanced Research Projects Agency，HSARPA）正式成立网络安全部门（Cyber Security Division，CSD）[15]。该部门的使命是提高关键信息基础设施和互联网的安全性和弹性，其具体职责包括：①开发和提供新技术和工具，帮助国土安全部和美国政府来保护当前和未来的系统、网络和基础设施；②引导和支持技术发展；③领导和协调包括政府机构、公共部门、私营部门及国际合作伙伴在内的研究与开发团体的网络安全研发工作。

CSD 自成立以来，开展部署了一系列网络安全项目，具体可参见[16]。接下来我们介绍其中几个与关键基础设施安全紧密相关的典型项目。

2.4.1　分布式拒绝服务防御

典型的分布式拒绝服务（Distributed Denial of Service，DDoS）攻击是指攻击者通过分布式拒绝服务攻击手段来向关键基础设施发送合理的服务请求，以此来占用其服务资源，进而使合法用户无法正常访问关键基础设施服务。金融机构、交通运输和能源行业的关键基础设施资源都可能遭受 DDoS 攻击。为了对 DDoS 攻击进行防御，CSD 设立了防御分布式拒绝服务（Distributed Denial of Service Defense，DDoSD）项目[17]。该项目主要目标是：①通过部署目前应对 DoS 攻击的最好实践方法（如 Best Current Practice 38—RFC 2827 网络入口过滤：抵抗基于 IP 源地址欺骗的拒绝服务攻击）来降低攻击者发送伪造数据包的能力。②为了让中等规模的企业能抵抗 1Tbps 的 DDoS 攻击，研发企业级安全应急沟通和协作处理工具。③将诸如“911”和下一代“911”等应急管理系统的服务容量扩充一倍，以此来应对基于手机接入的拒绝服务攻击。基于这些目标，该项目的具体研发内容包括：

1. 通过网络测量和验证分析来建立DDoSD最佳实践

在许多情况下,攻击者可以使用一个伪造的源地址发送网络数据包。例如,来自攻击者的数据包可能会被错误地解析为来自一个公司、组织或政府机构。大量的拒绝服务攻击依赖于使用伪造源地址。而且伪造源地址还增加了溯源工作的难度。现有的网络安全防护最佳实践技术能在网络外围筛选出伪造地址,并利用一些额外的扩展功能来应对更复杂的网络情况。这些防护技术可以有效地削弱那些基于伪造源地址技术的DDoS攻击。例如,源地址验证(Sender Address Verification,SAV)技术的广泛的部署就可以有效阻止源地址伪造。为此,2015年9月,DHS科学技术司(Science and Technology Directorate,S&T)资助了加州大学圣迭戈分校(University of California, San Diego,UCSD)130万美元,用于研究对互联网上使用的SAV技术进行评估和改进。

2. 沟通和协作工具

DDoS攻击的分布式特性为攻击者提供了几个优势。一般情况下,DDoS攻击者来自于不同组织被攻破利用的电脑主机。而且,随着网络带宽和计算能力的不断增加,攻击者的可利用资源变得越来越多。这些都有助于攻击者发起危害更严重的DDoS攻击。

2015年9月,DHS S&T资助了南加州大学信息科学研究所(University of Southern California, Information Sciences Institute, USC ISI)180万美元,用于研究在互联网服务提供商(ISP)和其他网络之间开发一个通用的接口,用以对网络通信的攻击进行诊断。这种称为软件定义的安全技术将允许终端用户在ISP中观察和控制自己的流量和路由,帮助他们预见DDoS攻击。USC ISI研究显示,30个部署了这一技术的领先的互联网服务提供商有效地消除了94%的DDoS攻击。

2015年9月,DHS S&T资助了科罗拉多州立大学270万美元,用于研究基于云计算服务的网络膜技术(NetBrane)。虽然云安全服务提供了一些DDoS保护,但目前的解决方案不能保证所有用户的安全。许多组织,如政府、军事和金融组织,需要严格管理他们自己的数据。这种数据管理方式与云计算中的数据管理方式是不一致的。然而,NetBrane却可以利用云计算服务的属性,允许用户在本地管理数据,有效地满足了用户本地管理数据的需求。

2015年9月,DHS S&T资助了俄勒冈大学计划创建一个网络“吊桥”(DrawBridge)项目来应对DDoS攻击。目前,因为网络使用者的数据是由互联

网服务提供商来管理的，因此各个用户不能自己管理他们的网络流量。在 ISP 流量接入点部署“吊桥”项目，将允许网络使用者与 ISP 密切合作以阻止不允许的异常网络流量。ISP 与用户之间的协调合作，将有利于缓解 DDoS 攻击。

由于现在的 DDoS 攻击规模巨大，中型组织很难单独应对 DDoS 攻击。因此，为了抵御这类攻击，2015 年 9 月，DHS S&T 资助了波兰的伽罗瓦公司 170 万美元，用于开发一个基于通信软件的 DDoS 响应解决方案。该方案将部署在多个组织中，以便各组织之间更好地协作。通过点对点共享软件对 DDoS 的攻击细节进行交流，使合作组织相互检测并进行统一防御部署，以此来抵御成千上万的 DDoS 攻击。

2015 年 9 月，DHS S&T 资助了维吉尼亚州的沃特福德威弗利实验室 62.9 万美元，用于研发可以防御 DDoS 的新技术和新工具。这一项目将完全开源。这个开源项目完成后，联邦政府组织、关键基础设施提供商和组织都将可以使用这一成果来开发可防御 DDoS 攻击的云服务。

3. 新颖的 DDoS 攻击缓解和防御技术

拒绝服务攻击新的变种会不断地在新的应用领域发起新的攻击。例如，2013 年初，国土安全部和联邦调查局就发出过关于在紧急救援管理服务系统(如 911 系统)中有可能发生拒绝服务攻击的安全警告。这些紧急救援管理服务系统包括移动警务设备，网络物理系统以及关键基础设施组件等，这些设备和系统都是拒绝服务攻击的潜在攻击目标。一般情况下，都是等发生了新的安全攻击之后，相应的安全响应才会给出安全应对措施，即安全响应都是反应式的。在理想情况下，最好的情况就是在发生大规模安全攻击之前，响应的安全应对技术或解决方案就已经准备好了，即安全响应是一种主动式的。因此，本研究内容的目标就是，针对那些还没有遭遇过大规模 DDoS 攻击的潜在目标，设计并制定 DDoS 安全防护机制。例如紧急救援管理服务系统和网络物理系统就是非传统的潜在攻击目标，而且这些都是容易遭受拒绝服务攻击的系统。

由于关键基础设施的数据中心与不同行业系统的正常运转密切相关，这些数据中心一旦遭受 DDoS 攻击，那么后果将比其他目标遭受攻击的后果更加严重。因此，2015 年 9 月，DHS S&T 资助了德拉瓦大学 190 万美元，用于研究针对关键基础设施数据中心的新型 DDoS 攻击的缓解和防御技术。

2.4.2 过程控制系统安全

过程控制系统(Process Control System，PCS)用于远程监视和控制关键基

础设施的敏感操作及物理状态。当这些网络隔离系统与企业网络集成之后，其潜在的安全漏洞或脆弱性可能就会暴露在公共网络上了。这些安全问题将促使PCS厂商、使用者和运营者加大对PCS安全防护机制的研究投入。大多数的关键基础设施厂商不是由联邦政府拥有的，而是由私营企业经营的。过程控制系统安全项目[18]由联邦政府资助给供应商们，以此来协助关键基础设施使用者和运营者加强安全防护措施。DHS S&T已经与石油、天然气及电力部门建立了紧密的合作，开展了以下项目：

(1) 将石油和天然气工业连接起来增强网络安全(Linking the Oil and Gas Industry to Improve Cyber Security，LOGIIC)[19]；

(2) 使得智能电网中的网络基础设施变得可信(Trustworthy Cyber Infrastructure for the Power Grid，TCIPG)[20]。

在16个国家关键基础设施行业中，发电厂、石油和天然气精炼厂及其管道等是较为重要的设施，如果它们的控制和数据系统遭受网络攻击，那么就有可能造成全国性的电力、石油或天然气供给瘫痪。由于美国85%至90%的关键基础设施是由私营企业掌控，因而政府要保证信息系统的安全并非易事。因此，2004年，国土安全部创建了LOGIIC项目，旨在加强油气企业间的联合研发、测试和评估工作，提高油气工业数字控制系统的网络安全等级，增强系统的安全防护措施。该项目的具体目的是研发减少油气工业控制系统安全漏洞或脆弱性的技术，然后验证这些技术，最后向石油和天然气公司推荐这些技术[20]。

LOGIIC[21]是由国土安全部资助，网络安全研究和开发中心拟定，加州SRI国际公司负责具体实施的。LOGIIC首次将政府、工业界、研究实验室、网络安全服务商和处理控制技术服务商等各方面的力量联合起来，创建了一个真实的油气控制系统测试平台。研究人员用计算机病毒、网络蠕虫和网络威胁技术来评估油气系统的安全等级，研究系统本身存在的安全漏洞及相应的防护机制。目前，LOGIIC已对下属多个项目进行了研究，并形成了最终报告，这些项目包括：安全仪表系统(Safety Instrumented Systems，SIS)项目[22,23]，主机保护策略(Host Protection Strategies，HPS)项目[24]，无线项目[25]，虚拟化项目[26]，远程监控项目[27]。

国家电力关键基础设施的正常运转依赖于电力系统中计算和通信网络的安全。计算和通信网络面临的安全威胁主要包括网络安全和物理破坏两方面因素。其中，网络安全因素主要是指攻击者通过获得电力系统的访问权，对电力系统进行拒绝服务攻击及其他网络攻击。物理破坏因素主要是指对电力系统的恐

怖袭击，自然灾害破坏或人为误操作等。因此，为了应对这些网络安全和物理破坏威胁，DHS S&T 和能源部联合资助了 TCIPG 项目，旨在解决国家电网安全防护中面临的挑战问题，改进国家电网建设方案，提高国家电网的网络和物理安全性和可靠性。在 TCIPG 项目中，超过 35 个工业界和学术界单位紧密合作，一起致力于研发和评估适用于安全智能电网的应用技术。该项目主要关注对电网系统中的底层通信和数据设备的安全防护，确保这些设备在正常运转时、发生网络安全攻击时及发生电力突发故障时都可以安全可靠地运行。

2.4.3　移动目标防御

目前，信息技术系统的配置是相对静止的。例如，地址、名称、软件栈、网络和各种配置参数等在很长一段时间内基本是保持不变的。这种静态配置方式是传统的信息技术系统为了设计简单而沿袭下来的，并没有考虑到静态配置信息被攻击者恶意利用的情况。然而，这些系统的静态特性为攻击者发起攻击提供了一个非常大的便利条件。例如，攻击者在发起攻击之前，依据系统的静态配置信息，可以有充足的时间来制定攻击策略和具体的攻击方法。为了应对这一威胁，CSD 建立了移动目标防御（Moving Target Defense，MTD）项目[28]，旨在研发一种系统动态配置能力、动态转换系统的状态和配置参数，增加系统运转状态的不确定性，以此来加大攻击者的攻击难度。此外，MTD 项目还试图开发具有弹性的系统硬件，即当系统遭受攻击时硬件仍可以保持其正常功能。

MTD 侧重于研究如何确保系统在遭受攻击的环境中仍能够安全运行。具体地，在发生网络攻击的情况下，MTD 将在多个系统维度上来控制系统配置状态的变化，增加系统的不确定性，增加攻击者对网络实施探测和攻击的成本，降低攻击成功率。表 2-9 给出了 MTD 关键技术的特点。

2.4.4　防御技术实验研究试验台

由于在操作系统及网络中检测恶意软件本身存在一定的安全风险，现有的网络基础设施和操作网络都无法满足这种需求。这就需要通过搭建一个网络安全试验平台来验证网络安全新技术。目前测试和验证新的安全技术只能在小到中等规模的研究实验室进行，这也就无法有效模拟大规模运营网络或互联网遭遇安全攻击的场景。为了应对这个问题，DHS 与美国国家科学基金会（National Science Foundation，NSF）合作，于 2004 年创建了防御技术实验研究（Defense Technology Experimental Research，DETER）试验台项目[30,31]。

表 2-9 MTD 关键技术特点[29]

结构层级	关键技术	特点
应用层	基于软件修改	针对某种具体的功能实现软件修改
	基于编译器	方便,依赖于自动编译器
网络层	自适应自同步动态地址转换(Adaptive Self-Synchronized Dynamic Address Translation,ASD)	变化简单,同步开销大
	突变网络(Mutable Networks,MUTE)	变化多样,不可预测。但保持网络中变化的同步性
	自清洗入侵容忍技术(Self Cleansing Intrusion Tolerance, SCIT)	配置变化较快
	基于 IPv6 的移动目标防御(Moving Target IPv6 Defense, MT6D)	地址空间大,变化多
IP 层	动态网络地址转换(Dynamic Network Address Translation, DyNAT)	可随机化 IP 地址,对抗中间人攻击,但不能发现终端主机的嗅探
	带有自我防御的应用(Applications that Participate in their Own Defense, APOD)	同时随机化 IP 地址与端口,不透明
	网络地址空间随机化(Network Address Space Randomization, NASR)	局域网级别的 DHCP 更新,主要是防范 hitlist worms 威胁
	随机主机突变(Random Host Mutation, RHM)	不需改变终端主机配置,开销较大
	开放流随机主机突变(OpenFlow Random Host Mutation, OF-RHM)	透明,开销小,但不能用于传统网
指令与数据层	指令集随机化(Instruction Set Randomization, ISR)	能阻止漏洞扩散,需要硬件支持
	地址空间随机化或地址空间布局随机化(Address Space Randomization or Address Space Layout Randomization, ASLR)	可利用硬件实现快速加密

1. DETER 简介

DETER 实验室(DEfense Technology Experimental Research Laboratory, DETERLab)是为研究和定义大规模 DDoS 测试床而设立的。该实验室主要有三个任务:①设计、构建和操作具体支持安全研究的网络测试床;②研发软件工具来帮助创建、监控和分析复杂的 DETERLab 安全实践;③促进建立一个安全研究的协作型联盟,例如,互联网安全技术评估方法(Evaluation Methods for Internet Security Technology, EMIST)项目就是由宾夕法尼亚州立大学、McAfee 实验室、国际计算机科学研究所(International Computer Science Institute, ICSI)、普渡大学、SPARTA 公司、斯坦福国际研究院(SRI International)和加州大学戴维斯分校共同承担。

DETER 项目主要是将 DETER 测试床开发成先进的科学仪器,用以提高网络安全的科学性。主要实现以下三个目标:①推动网络安全实验的研究工作,在测试床上可以进行科学严谨并且可重复的实验;②发展先进的测试床技术,主要包括测试床联合技术和实验管理技术;③共享基础设备资源,扩大用户范围和数量。一方面,通过共享数据、代码、结果,创立知识社区等方式来共享测试床的基础设备资源。将测试床使用变得更加简单和自动化,方便用户使用。另一方面,在教育领域发展实验床,扩大用户数量和范围。发展先进的测试床技术,能够进行鲁棒性、多样性以及弹性实验。

DETER 测试床共有 400 多个节点,包含两部分:一半在南加州大学信息学院,另一半在加州大学伯克利分校。DETER 测试床使用的是美国犹他州立大学的一种被称为“Emulab”的集群测试技术。Emulab 技术[32]可以为研究人员开发、调试和评估系统提供多种环境的网络测试环境。测试床中的每个节点都是一个具有大容量硬盘存储、2GB 内存的 PC 机,并且通过 4 个 10/100/1000 Mbps 的以太网连接到可编程的背板上。在实验脚本的控制下,Emulab 控制软件自动地部署节点并且设置连接。在实验中,用户可以使用服务器上的 Web 界面通过控制面板查看节点,重新加载节点,或者退出实验。当别的节点失效时,用户还能够手动重启。用户可以通过串口控制台进入节点,也可以通过用户服务器连接控制端口。

2. DETER 测试床目前进行的项目

表 2-10 给出了目前在 MTD DETER 测试床上开展的项目名称及其归属单位。

表 2-10 MTD DETER 测试床目前进行的项目

序号	项目名称	归属单位
1	油气/天然气管线的 SCADA 安全	西南交通大学
2	新网络体系结构的层次分类	加州大学(伯克利)
3	Dos 限制的网络体系结构	加州大学(尔湾)
4	恶意软件分析的大规模测量	加州大学(伯克利)
5	使高年级学生能够将理论知识用于实验的网络安全实验室	约旦科技大学
6	将计算分配到志愿节点的平台	南加州大学
7	安全的 DDoS 保护框架	东京大学
8	云计算的访问控制，一个能够教育和指导硕士博士研究生的研究方向	开罗大学工程学院电子和通信工程系
9	自适应 DDoS	斯坦福国际研究院
10	利用公共云处理 TCP 限制	加州大学(伯克利)
11	先进的计算机安全	国立科学技术大学
12	先进的持续威胁分类	Barnstormer Softworks, Ltd
13	AHcourses	巴伊兰大学(以色列)
14	实验分布式确定性操作系统	耶鲁大学
15	修改比特流的 P2P 客户端通信模式分析	布宜诺斯艾利斯大学
16	匿名消息协议和系统	巴伊兰大学(以色列)
17	应用层攻击检测归因和消减系统	加州大学圣巴巴拉分校
18	应用加密和网络安全课程	罗德福德大学
19	安全操作系统的体系结构	纽约州立大学约翰杰学院
20	OSPF 协议规范的安全评估	以色列理工学院
21	攻击分类	Thiagarajar College of Engineering
22	攻击检测和对策仿真	海峡大学(土耳其)
23	关键基础设施系统的自动入侵检测和响应系统	阿肯色大学布拉芙松分校
24	路由避免的测量项目	加州大学(洛杉矶)计算机科学系
25	消减网络安全风险的行为研究	圣荷西州立大学

续表

序号	项目名称	归属单位
26	网关边界协议(BGP)路径验证安全	龙研究实验室
27	BGPSEC 执行测试	斯巴达公司,帕森斯公司
28	生物启发安全计算	匹兹堡大学
29	基于网络流量分析的僵尸网络检测	丹麦技术大学
30	Bro-ids 性能评价	坎皮纳斯州立大学(巴西)
31	CCTF 课程支持	波莫纳加州州立理工大学
32	僵尸网络表征	喀拉拉大学计算机科学系(印度)
33	关键基础设施安全研究(CISR)	南伊利诺伊大学爱德华兹维尔分校
34	Class account for CSE952 course at UNL	内布拉斯加林肯大学
35	Class Project for CSC 453	南康涅狄格州立大学
36	Clearing house for the TIED GENI prototyping project	南加州大学信息科学研究所
37	云辅助路由	内华达大学雷诺分校
38	群集航天器仿真	美国宇航局(NASA)艾姆斯研究中心
39	cmrex	南加州大学
40	网络防御的认知助手	乔治梅森大学
41	JPL 的协作支持(Collaborative support for JPL)	南加州大学
42	科罗拉多州课程 CS356(Colorado State Course CS 356)	科罗拉多州立大学
43	移动目标防御的指挥和控制	佛罗里达人机认知研究所
44	折中的实体检测	本古里安大学(以色列)
45	计算机入侵检测	约翰・霍普金斯大学
46	计算机科学 161-计算机安全	加州大学(伯克利)
47	计算机安全体系结构	霍普斯金大学信息安全研究所
48	计算机安全分类	圣路易斯大学
49	执行安全相关任务	Dr. V. Radha

续表

序号	项目名称	归属单位
50	波兰特大学计算机系统安全课程实验室	波兰特大学
51	为学生课程创建实验室	肯尼索州立大学
52	CS3210 课程项目:软件安全入门	鲍灵格林州立大学
53	CS460 安全通信课	波莫纳加州州立理工大学
54	CS556 科罗拉多州立大学研究生计算机安全课程	科罗拉多州立大学
55	CS153 计算机安全课	菲律宾大学
56	CS283 范德比尔特的计算机网络	范德比尔特大学
57	CS298 特殊项目	菲律宾大学
58	CSCI 6642	博伊西州立大学
59	CSCI551-Spring2014	南加州大学信息科学研究所
60	CSE403 Grad Security Course	西交利物浦大学
61	CSI Miniproject	维拉诺瓦大学
62	CSU-CS557-Spring2014	科罗拉多州立大学
63	网络攻击	德州理工大学
64	网络入侵检测	福德姆大学
65	智能电网的网络物理系统安全	艾奥瓦州立大学
66	网络安全课程	南弗吉尼亚社区学院
67	网络路径	沃福德学院
68	网络安全	马德里理工大学(西班牙)
69	网络安全第二顶石课程(Cybersecurity Capstone Ⅱ)	纽约州立大学约翰杰学院
70	网络安全课	肯塔基大学
71	Cypress	华盛顿州立大学
72	DASH	南加州大学信息科学研究所
73	DDoS 蠕虫基线数据	BIT
74	DDoS-AE	Blue Ridge Envisioneering/DHS
75	安全网络协议声明的网络技术(Declarative networking techniques for securing network protocols)	宾夕法尼亚大学

续表

序号	项目名称	归属单位
76	DeepSky	佛罗里达大学
77	DDoS 攻击防御	尼赫鲁科技大学(印度)
78	防御 DDoS	匹兹堡大学
79	点对点网络的设计与实现	圣克劳德州立大学
80	为学生学习 Web 应用程序漏洞的网站设计	塔斯基吉大学
81	Detecting compromised machines	佛罗里达工业与机械大学
82	使用机器学习技术检测 DDoS 攻击	度库兹埃路尔大学(土耳其)
83	DDoS 检测	西北工程技术学院(印度)
84	基于熵的 DDoS 攻击检测	特里布文大学工程研究所(尼泊尔)
85	DETER SPI 开发	南加州大学维特比工程学院资讯科学研究院
86	DETER-GENI-TASK2	北卡罗来纳州立大学
87	DetMACRO	加州大学(戴维斯)
88	为网络安全和网络实验开发实验工作台	南加州大学
89	Differentiating between distributed pulsating denial of Service attacks and flash crowds	扎皮大学信息技术研究所
90	Digital Ants project for Bio-Inspired Cyber Security Research	西北太平洋国家实验室
91	DIPS-Mon：Data Integrity Protection through Security Monitoring for Just-in-Time News Feeds	密苏里大学
92	分布式计算	艾瑞尔大学
93	DISTRIBUTED COMPUTING COURSE	华盛顿州立大学
94	分布式 DDoS 攻击防御	印度标准学会
95	电网的多元化网络安全	霍华德大学
96	Early filtering of unwanted traffic	南卡罗来纳大学
97	Educational Project	埃及不列颠大学
98	EE 599：Cybersecurity	肯塔基大学

续表

序号	项目名称	归属单位
99	Enabling Open Flow in DETER	南加州大学信息科学研究所
100	Enhanced Hadoop for Bioinformatics	南加州大学信息科学研究所
101	通过预防 DoS 攻击保证可用性	克什米尔大学
102	Ensuring reliable，timely communication over network-DoS-prone link	巴伊兰大学(以色列)
103	道德黑客	博伊西州立大学
104	评估 DoS 防御	巴伊兰大学(以色列)
105	Evaluation of CCNx robustness against DDoS attacks	加州大学(洛杉矶)
106	Flood Watch DDoS Defense	南加州大学信息科学研究所
107	for my cloud seminar class	南加州大学
108	FPGA Accelerated Intrusion Detection System using NetFPGA node	南加州大学信息科学研究所
109	FRADE	印度标准学会(ISI)
110	未来具有安全功能的互联网实验床	里约热内卢联邦大学
111	Graduate Class on Cryptography and Network Security	维拉诺瓦大学
112	Hands-on labs for Network Security course	德州农工大学
113	Hardware Enabled Zero Day Protection	Def-Logix，Inc.
114	Harvey Mudd College CS125 Networking	南加州大学信息科学研究所
115	HU Security Class	哈希姆大学
116	Illustrate and develop attacks against DNSSEC	信息科学研究所
117	Implementation and mitigation of DDoS attacks on a server	德里理工大学
118	Implementing state machine replication for Wide-Area Networks	淡江大学(台湾)
119	Incast	特拉维夫大学(以色列)
120	INCS-620	纽约理工学院
121	信息安全	南康涅狄格州立大学

续表

序号	项目名称	归属单位
122	Install PNNL GridLAB-D in DETERlab	南加州大学信息科学院
123	Installing the Skaion Traffic Generation System on DETER	加州大学(伯克利)
124	Integrated Simulation and Emulation Platform for Security Experimentation	范德堡大学
125	智能僵尸网络检测方法	坎皮纳斯州立大学
126	Internal instructors project	印度标准学会
127	Introduction to Computer Forensices	加拿大国王大学学院
128	Intrusion Detection Class	约翰·霍普金斯大学
129	Intrusion-Tolerant SMR and Storage Protocols	达姆施塔特工业大学(德国)
130	IPv6 Security and Conformance	FreeBSD Project
131	IRON	Raytheon BBN Technologies, Inc(雷神技术公司)
132	IST Network Security Arena	密西西比西南社区学院
133	IT Security & Forensics(IT 安全和取证)	特鲁罗彭威斯学院
134	IT@iTech	伊莫卡利技术学院
135	IUCC-Test	大学之间计算中心(以色列)
136	JHUISI-Security Research Testbed	约翰·霍普金斯大学
137	JPL Research & Technology Development	喷气推进实验室
138	KUL	金斯顿大学(英国)
139	Lab Experiments as part of USC Computer Security Systems Course	南加州大学
140	Lab sessions for network security course-graduate level	维拉诺瓦大学
141	Labs for CS6823	纽约大学理工学院
142	LACREND	南加州大学/信息科学研究所
143	Learn2Secure	孟菲斯大学
144	低强度 DDoS 攻击检测评估	威灵顿维多利亚大学

续表

序号	项目名称	归属单位
145	Maestro	洛克希德·马丁公司
146	在 DETER 中映射国家电网网络 Mapping PowerGrid network in DETER	南加州大学,信息科学研究所
147	测量 DDoS 的细微迹象	日本国家信息通信技术研究所
148	midonet	网络虚拟化公司
149	Mobility First Future Internet Architecture Project→Computing layer design and implementation	杜克大学
150	Mosaic：Policy Homomorphic Network Extension	耶鲁大学
151	Nerdsville Security	Nerdsville，L. L. C.
152	NetPAC aims to provide context and situational awareness in the cyber domain by understanding the mission contribution of cyber assets and projecting the impact of cyber attacks	21CT，Inc.
153	网络同步	南加州大学,信息科学研究所
154	Network and Computer Security Class	科罗拉多大学
155	Network Processor Design and Programming	南加州大学,信息科学研究所
156	Network Processor Programming and Design	南加州大学,信息科学研究所
157	Network Security	马里兰大学学院分校
158	Network Security	扎皮大学信息技术研究所
159	Network Security Course	里海大学
160	network security course project	肯萨斯市密苏里大学
161	Network Security Coursework	华盛顿州立大学
162	Network Security Projects for CS 1153	俄克拉荷马城社区学院
163	network security projects for students in my classes	俄克拉荷马城社区学院
164	Network Security Techniques course	组织科学学院

续表

序号	项目名称	归属单位
165	New Experiment	加州多明戈山州立大学
166	NNSOA Botnet Detection	密苏里州立大学
167	NS-Spring 2015	FAST-National University of Computer & Emerging Sciences
168	NUS Project	新加坡国立大学
169	Optimal Design of Cyber Experiments	俄亥俄州立大学
170	Overlay-based DDoS Defense System	哥伦比亚大学计算机科学系
171	P2P 僵尸网络流量分析与检测	格拉斯哥喀里多尼亚大学(英国)
⋮	⋮	⋮

2.5 其他典型项目

2.5.1 国家基础设施保护计划项目

1. 项目简介

早在 2006 年，国土安全部就已发起了国家基础设施保护计划(National Infrastructure Protection Plan，NIPP)[33]。NIPP 的目标是通过加强对国家关键基础设施和核心资源的保护，来建立一个物理上、信息网络上更安全以及故障恢复能力更强的美国，以此来阻止、减缓或消除由恐怖袭击所带来的蓄意破坏影响，加强国家在袭击、自然灾害或突发等事件中的预防、及时响应和快速恢复的能力。为了实现这些目标，NIPP 要求实现以下具体目标：①共享恐怖袭击和其他灾难危害事件的信息；②实现一个长远规划的风险管理系统；③最大化核心资源的使用效率。

其中，关于风险管理系统，NIPP 也进一步给出了一个如图 2-19 所示的基本框架。框架中包含三种关键基础设施元素，即物理设备、网络空间、人。涉及 6 个主要环节，即设定目标、识别认定基础设施、风险评定和分析、风险管理系统具体实现、有效性测试。

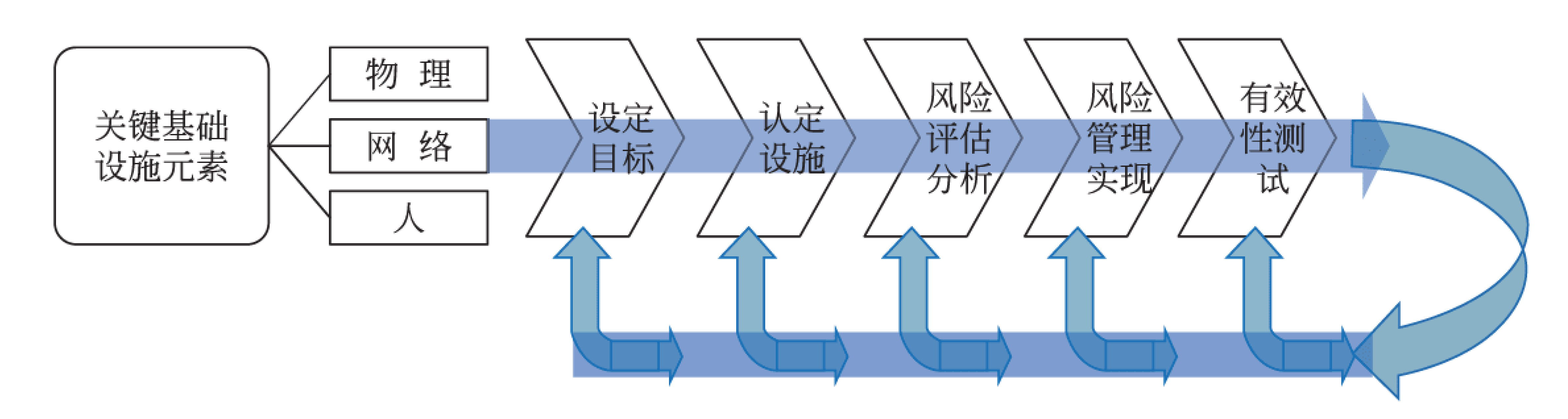


图 2-19　NIPP 关键基础设施安全和恢复基本框架图

NIPP 的愿景、任务、目标和核心原则分别为：

（1）NIPP 愿景

通过减少漏洞，最小化安全代价，增强对安全事件的识别、响应与恢复能力，使物理/网络关键基础设施保持安全性、稳定性与弹性。

（2）NIPP 任务

通过关键基础设施共同体的合作与协调，对关键基础设施中的物理/网络风险进行管理，以此增强关键基础设施的安全性、稳定性与弹性。

（3）NIPP 目标

对关键基础设施当中的威胁、漏洞和后果进行评估和分析，并据此开展风险管理活动；降低关键基础设施的运行风险，确保运行过程中的人身、财产、网络安全；通过预先制定安全预案、及时应急响应及快速恢复等方式，使事故造成的负面影响达到最小化，以此增强关键基础设施的弹性；在关键基础设施共同体当中增强信息分析能力，在面临安全风险时提高管理者的决策能力。

（4）核心原则

NIPP 当中建立了七个核心原则，从国家、区域、州、地区、部落、地方（State，Local，Tribal，and Territorial，SLTT）、所有者和经营者层面，为增强关键基础设施的安全性和弹性的各项规划与行动提供指导。具体地，①在关键基础设施的安全性和弹性建设方面，全面协调分配核心资源；②加强理解跨部门的相关性和相互依赖性（如图 2-20 和表 2-11 所示），加深认识安全风险，增强关键基础设施的安全性和弹性；③在关键基础设施共同体中及时分享安全事件信息；④在关键基础设施部门之间，对各个部门的优势资源进行比较、整合，实现合作共赢；⑤发展区域和 SLTT 伙伴关系，构建信息共享机制，提高关键基础设施安全性和弹性；⑥对于某些关键基础设施，需要与国际社会合作，签署跨境协作、互助及其他合作协议；⑦在安全性和弹性设计中，应综合考虑资产、系统和网络等一系列因素。

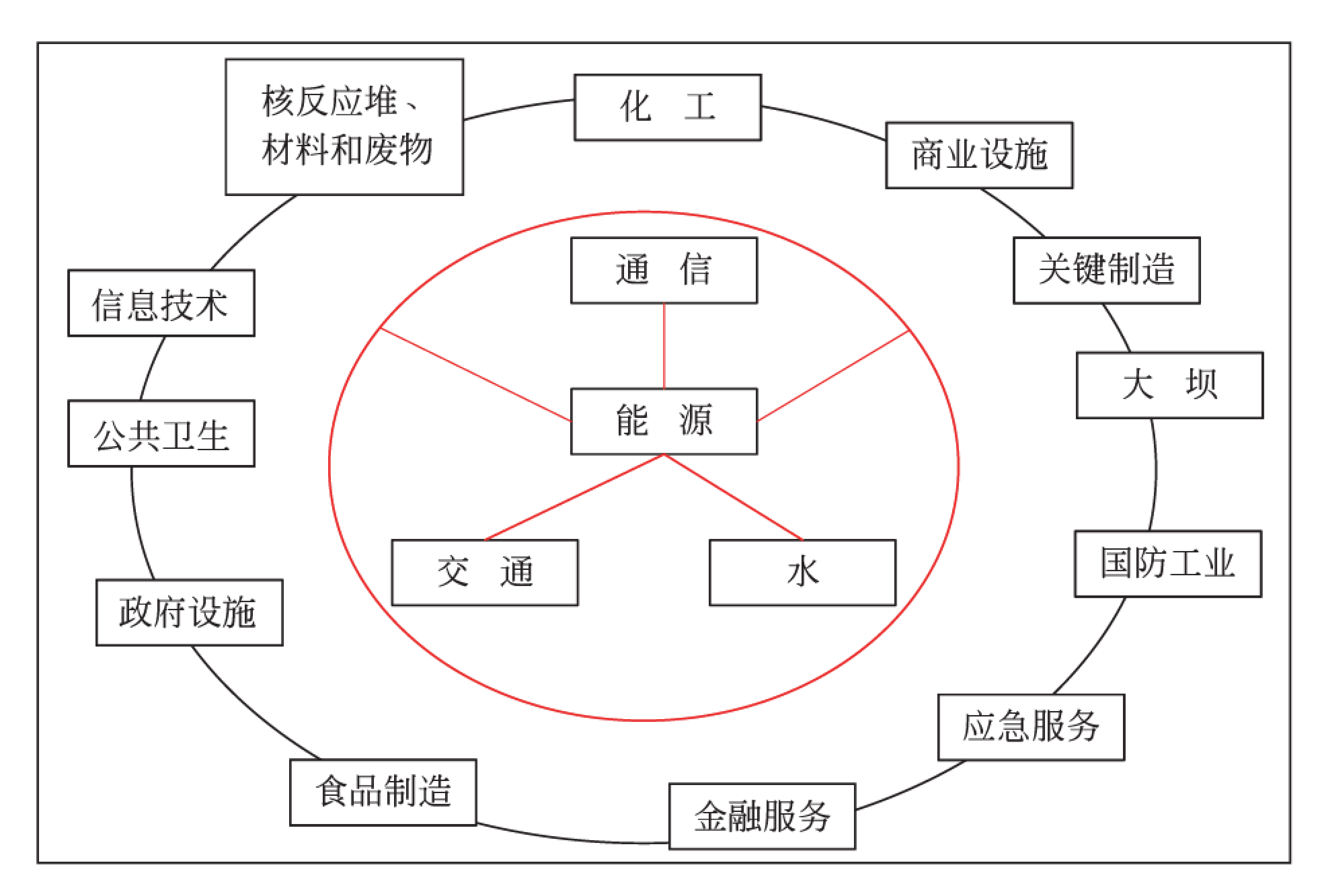


图 2-20 关键基础设施相互依赖关系

表 2-11 关键基础设施部门的相互依赖性

部门＼部门	石油/天然气	电力	交通	水	通信
石油/天然气	—	为发电厂的发电机提供操作燃料	为交通工具提供燃料	为水泵和水处理装置提供燃料	维持设备温度；为备用电源提供燃料
电力	为提取和传输设备（泵、发电机）提供电能	—	为高架交通线路提供电能	为水泵和水处理装置提供电能	为发射塔和其他传输设备提供电能
交通	运送物资/劳动力	运送物资/劳动力	—	运送物资/劳动力	运送物资/劳动力
水	生产用水	生产用水、冷却用水	交通工具操作、冷却用水	—	设备用水、清洁用水
通信	破损和泄漏检测、远程控制操作	检测和维护操作和电气传动	对车辆、铁路和公路货运进行确认与定位，提供用户服务信息	检测和控制水的供应和质量	—

此外，NIPP对美国的16个基础设施行业进行了脆弱性评估，并出具了相关报告，这些部门包括：化工、商业设施、大坝（水坝）、应急服务、金融服务、政府设施、信息技术、交通、通信、关键制造、国防工业、能源、食品制造、公共卫生、核反应堆，材料和废物、供水/污水处理行业。这些行业之间存在着相互依赖的关系，需要一种跨行业跨部门协调的管理方式，具体管理结构如表2-12所示。

表2-12　关键基础设施管理结构

<table>
<tr><th rowspan="2">基础设施行业</th><th rowspan="2">主管机构</th><th colspan="5">关键基础设施合作咨询委员会</th></tr>
<tr><th colspan="2">部门协调委员会（Sector Coordination Council SCC）</th><th colspan="2">政府协调委员会（Government Coordination Council GCC）</th><th>区域联盟</th></tr>
<tr><td>化学行业</td><td rowspan="8">国土安全部</td><td>√</td><td rowspan="16">关键基础设施跨部门委员会</td><td rowspan="16">联邦高级领导委员会</td><td rowspan="16">州、地方政府、部落协调委员会(State, Local, Tribal, and Territorial Government Coordinating Council, SLTTGCC)</td><td rowspan="16">区域联合协调委员会</td></tr>
<tr><td>商业设施行业</td><td>√</td></tr>
<tr><td>水坝行业</td><td>√</td></tr>
<tr><td>应急服务行业</td><td>√</td></tr>
<tr><td>通信行业</td><td>√</td></tr>
<tr><td>关键制造业行业</td><td>√</td></tr>
<tr><td>信息技术行业</td><td>√</td></tr>
<tr><td>核反应堆，材料，废料处理行业</td><td>√</td></tr>
<tr><td>金融服务行业</td><td>财政部</td><td>使用单独的协调体系</td></tr>
<tr><td>政府设施行业</td><td>国土安全部
总务管理局</td><td>不包含SCC</td></tr>
<tr><td>防御工业基础行业</td><td>国防部</td><td>√</td></tr>
<tr><td>能源行业</td><td>能源部</td><td>√</td></tr>
<tr><td>粮农行业</td><td>农业部
卫生部</td><td>√</td></tr>
<tr><td>公共卫生行业</td><td>卫生部</td><td>√</td></tr>
<tr><td>运输系统行业</td><td>国土安全部
交通部</td><td>SCC由运输方式分类</td></tr>
<tr><td>供水/污水处理行业</td><td>环境保护局</td><td>√</td></tr>
</table>

2. 关键领域未来规划

根据 NIPP 的总体规划，各基础设施部门也分别提出了各自的未来规划。以下重点针对金融、交通、能源（包括石油、天然气、电力）、通信等领域的未来规划的目标和相应措施以图表的形式进行介绍。

（1）金融领域

金融领域的未来规划目标和措施如表 2-13 所示。

表 2-13　金融领域的未来规划目标和措施

信息共享	
目标 1	实现和维护结构化程序，共享与网络和人身安全相关的信息。在企业、各部门的行业、私营部门和政府中，分析安全威胁及安全漏洞
措施	在行业内、跨行业、行业与政府间，加强安全威胁与趋势信息共享
	通过与其他关键基础设施部门和国际合作伙伴的信息共享，建立各部门间的相互依赖关系
	通过结构化信息共享过程和路径，加速信息共享
最优方法	
目标 2	提高整个金融服务行业和服务提供商的风险管理能力和企业的安全防护能力
措施	促进 NIST 的网络安全架构的广泛应用
	鼓励发展和使用第三方风险管理的最优方法
事件反应和恢复	
目标 3	与国土安全、执法和情报社区、金融监管当局、其他工业行业和国际合作伙伴合作，以在重大安全事件中进行及时的响应和应急恢复
措施	将应对事件的机制和过程进行精简、社会化
	加强锻炼政府和私营部门的事件响应过程
目标 4	通过政府和行业之间的协调，讨论政策和监管措施，促进基础设施的安全性和弹性
措施	确定并支持能够提高关键金融基础设施的安全性和弹性的政策
	鼓励公司、金融监管机构和执行分支机构之间的密切协调，努力发展政策

（2）交通领域

交通领域的未来规划目标和措施如表 2-14 所示。

表 2-14 交通领域的未来规划目标和措施

序号	目标	措施
1	管理关键交通基础设施中的物理、人和网络要素的安全风险	• 提高针对恐怖袭击的应对能力及恢复能力 • 推进关键运输业务的网络系统的安全态势感知能力
2	利用运输系统部门的响应、恢复和协调能力，以支持整个社区的弹性(可恢复性)	• 加强关键交通基础设施的准备工作，以增强应对所有危险的恢复能力 • 为救援人员和基础设施的维修队伍提供帮助 • 扩大合作伙伴关系，提高社区和相互依存部门的弹性
3	在部门、司法管辖区和学科之间实施有效的协作，加强公共部门和私营部门之间信息的共享	• 优化跨部门，司法管辖区，学科和公共和私人利益相关者之间的信息共享流程 • 改善和扩大伙伴关系，包括相互依存的部门和州、当地、部落和区域的合作伙伴 • 通过支持一个全国性的报告机制，加强运输安全和安全问题的报告、分析和传播
4	加强全球运输系统的所有灾害防备和应变能力，以维护美国的国家利益	• 扩大以风险为基础的安全方法，包括风险分割，以对出入美国的人和货物进行确认和管理 • 增强全球供应链的弹性

(3) 能源领域

能源领域的未来规划目标和措施如表 2-15 所示。

表 2-15 能源领域的未来规划目标和措施

风险管理			
风险识别		能源部门风险控制	
目标 1	对关键基础设施的威胁、漏洞和后果进行评估与分析，并进行风险管理	目标 2	通过可持续努力，降低风险，保障关键基础设施当中的人身、物理、网络威胁，并对安全投资的成本和收益进行解释

续表

<table>
<tr><th colspan="4">风险管理</th></tr>
<tr><th colspan="2">风险识别</th><th colspan="2">能源部门风险控制</th></tr>
<tr><td rowspan="5">措施</td><td>加强能源产业的网络-物理集成能力</td><td rowspan="5">措施</td><td>网络安全：签署 EO 13636-“提高关键基础设施网络安全”</td></tr>
<tr><td>加强能源基础设施的可靠性，发展网络安全解决方案</td><td>物理安全性和弹性：改进自然环境研究委员会（Natural Environment Research Council，NERC）可靠性标准、建立工业电气设备共享项目</td></tr>
<tr><td>对电网可靠性的未来挑战进行确认与准备</td><td>自然灾害和气候弹性：签署 EO 13653-“为气候变化的影响做准备”、建立 climate. gov，以提高公民意识</td></tr>
<tr><td>对其他关键基础设施领域进行协助，以确定它们对能源部门的依赖性</td><td rowspan="2">发展劳动力：提升劳动力的职业技能，制定劳动力准入机制</td></tr>
<tr><td>加强与关键的基础设施供应商的联系，促进双方的支持与交互</td></tr>
<tr><td colspan="4">信息共享与通信</td></tr>
<tr><td>目标 3</td><td colspan="3">在关键基础设施领域及其社区分享可操作的相关信息，建立风险意识，改进相关决策</td></tr>
<tr><td rowspan="2">措施</td><td colspan="3">建立国土安全信息网络（Homeland Security Information Network，HSIN）：一个能够在各个层面提供安全事件信息共享的平台</td></tr>
<tr><td colspan="3">建立信息共享分析中心（Information Sharing and Analysis Center，ISAC）：信息共享和威胁情报分析平台</td></tr>
<tr><td colspan="4">关键基础设施弹性与防范措施</td></tr>
<tr><td rowspan="2">目标 4</td><td colspan="3">通过最小化负面后果、建立事件推进计划和缓解措施、有效地拯救生命和保证基本服务快速复苏的计划，提高关键基础设施弹性</td></tr>
<tr><td colspan="3">在演习与实际事件的过程与善后当中，加强技能学习与适应</td></tr>
<tr><td rowspan="2">措施</td><td colspan="3">通过能源部部署资源，协助恢复能源系统，提供初始联络点</td></tr>
<tr><td colspan="3">基于地理的能源信息分析环境（Environment for Analysis of Geo-Located Energy Information，EAGLE-I）：提供对能源基础设施的监视功能</td></tr>
</table>

（4）通信领域

通信领域的未来规划目标和措施如表 2-16 所示。

表 2-16 通信领域的未来规划目标和措施

序号	目标	措施
1	保护和提高通信设施的整体物理和逻辑健康	• 对主干网进行防护 • 在为有关人员提供通信资产的过程中，标准化筛选过程 • 对访问控制和内部威胁缓解进行实践操作 • 在产业和政府之间，促进关于威胁和脆弱性的信息共享
2	在关键通信服务中断事件当中迅速重建，并减轻级联效应	• 设立一系列程序与规程，以迅速应对危机当中对通信基础设施的影响，并保证危机期间基础设施的继续运作(Continuity of Operations，COOP)能力
3	提高部门的国家安全和应急准备能力，与联邦、州、地方、部落、国际和私人部门合作，以降低风险	• 针对各方面威胁进行模拟和演习的开发，并参与到其中 • 发展教育项目，增强通信技术培训，对紧急情况下潜在的薄弱环节进行学习 • 在相关服务项目当中，参加会议、展会和推广活动 • 开发和参与跨部门威胁练习 • 开发和参与跨部门的工作小组

3. 2016 年 NIPP 发展与实施目标

美国国土安全部发布《国家基础设施保护计划安全性和弹性的挑战》[34]，确定了在 2016 年度，在 NIPP 安全性与弹性方面需要解决的一系列挑战，并提出了发展与实施目标。

(1) 美国州际天然气协会——改善网络威胁信息共享

目标：促进和鼓励关于网络威胁信息的自动共享。

(2) 湾区灾难恢复中心——建立工具箱，增强区域内基于风险的跨部门决策能力，提升关键基础设施安全性和弹性

目标：将可定制、可扩展的产品进行集成，建立工具箱，增强跨部门的信息共享和决策能力，提高区域关键基础设施安全性和恢复力。

（3）美国自来水厂协会——提高美国中小水务系统的网络安全

目标：提供免费实验场地，为水务行业管理者和经营者提供网络资源。利用这些资源，发现网络安全漏洞，并制定详细、可行的安全防护措施来解决这些漏洞。

（4）芝加哥通过团队合作来培育工业安全性与弹性（Chicago Fostering Industry Resilience and Security through Teamwork，ChicagoFIRST）的计划——建立区域联盟安全门户网站

目标：开发一个门户网站和工作区，为关键金融行业公司与公共部门机构提供联系，以在紧急情况发生时获取安全事件信息。该系统包括应急操作程序、消息传递系统，以及物理安全、网络安全和监管团队。

（5）防灾联盟——构建公共区域灾难恢复框架

目标：构建敏感信息共享的发展框架，以增强地区灾难中的响应机制，提高灾后恢复能力。

（6）飞马项目——建立一个全国性的危机事件响应、恢复和访问流程标准

目标：开发一个危机事件响应、恢复和访问流程标准，加强与紧急服务部门工作协调委员会的合作，增强各部门在危机事件中的准备和响应能力。

2.5.2　下一代网络基础设施项目

1. 项目简介

国土安全部科学技术司和金融行业从业者意识到，金融领域关键基础设施面临着三大挑战：①攻击者在我们未察觉的情况下，一直在渗透攻击我们的金融系统和网络；②金融领域非网络安全部门的从业人员对自身系统和网络的安全态势理解不准确，不够全面，往往是安全事件发生以后才发觉；③金融网络运营者缺乏网络安全应急响应和消除安全攻击的技能。

因此，国土安全部科学技术司创建了下一代网络基础设施（Next Generation Cyber Infrastructure，NGCI）项目，该项目隶属于顶点（Apex）项目[35]。旨在提供一系列金融服务行业的先进安全技术和工具，以应对针对美国网络系统的攻击。NGCI 致力于为金融部门提供五个主要功能：

（1）动态防御

当前，利用不断变化的内部和外部网络结构，增加敌人对网络布局进行探测、攻击和利用的难度。然而，这种方式也可能因为一个潜在的攻击者，而大大增加了安全防护的经济成本。

（2）网络描述

对各资产的内部通信模式提供实时的网络分析，在网络事件中提供及时异常检测和快速反应的能力。

（3）恶意软件检测

提高检测和防御恶意软件的能力，对可能的恶意软件代码的变种进行预测。

（4）软件质量保证

降低误判率，加快分析时间，在复杂的软件代码中增加发现软件缺陷的可能性。

（5）内部威胁

在网络层之下检测是否存在数据泄露的可能，对潜在的内部威胁进行预测和安全建模。

2. 技术路线及项目规划

NGCI 利用现有的联邦政府资助和私营部门企业的研究工作，提供所需的功能。技术开发方法灵活、可重复，有 5 个不同的阶段[36]：

（1）搜寻候选技术。

根据网络顶点审查组(Cyber Apex Review Team，CART)提出的安全需求，对候选技术进行包括工业活动、技术浏览、技术过渡到实践等分析筛选工作。

（2）技术评估

使用 CART 成员定义的表征体系结构，对候选技术进行演示、测试和评估。

（3）系统开发与测试

进一步在公司测试环境中对产品进行测试和评估。在整个过程中，CART 全程参与并反馈意见，使用“建立-测试-重复”模型，进行系统开发和测试。

（4）系统集成

基于测试和评估结果，根据需要，对技术产品进行集成和完善。

（5）产业化

通过金融机构、管理安全服务提供商或风险资本的内部操作，制定和实施适当的过渡或商业化策略，建立支持模型，提供开源选项。

参考文献

[1] DHS. Department organizational chart. https://www.dhs.gov/organizational-chart

[2] DHS. Cyber storm: securing cyber space. https://www.dhs.gov/cyber-storm

[3] DHS National Cyber Security Division. Cyber storm exercise report. 2006. https://www.dhs.gov/sites/default/files/publications/Cyber Storm I After Action Final Report.pdf
[4] DHS Office of Cybersecurity and Communications & National Cyber Security Division. Cyber storm Ⅱ final report. 2009. https://www.dhs.gov/sites/default/files/publications/Cyber Storm Ⅱ Final Report.pdf
[5] DHS Office of Cybersecurity and Communications & National Cyber Security Division. Cyber Storm Ⅲ final report. 2011. https://www.dhs.gov/sites/default/files/publications/CyberStorm Ⅲ FINAL Report.pdf
[6] DHS Office of Cybersecurity and Communications & National Cyber Security Division. Cyber storm Ⅳ final report. 2015. https://www.dhs.gov/sites/default/files/publications/Lessons Learned from Cyber Storm Ⅳ.pdf
[7] DHS Office of Cybersecurity and Communications & National Cyber Security Division. Cyber storm Ⅳ final report. 2016. https://www.dhs.gov/sites/default/files/publications/CyberStormV_AfterActionReport_2016v Final-508 Compliant v2.pdf
[8] CSSP. Recommended practice: improving industrial control systems cybersecurity with defense-in-depth strategies. US-CERT Defense In Depth (October 2009), 2009
[9] ICS-CERT. ICS-CERT year in review, 2010
[10] CSSP. CSSP year in review, 2011
[11] ICS-CERT. ICS-CERT year in review, 2012
[12] ICS-CERT. ICS-CERT year in review, 2013
[13] ICS-CERT. ICS-CERT year in review, 2014
[14] ICS-CERT. ICS-CERT year in review, 2015
[15] Cyber Security Division. https://www.dhs.gov/science-and-technology/cyber-security-division
[16] CSD. CSD Projects. https://www.dhs.gov/science-and-technology/csd-projects
[17] CSD. Distributed denial of service defense. https://www.dhs.gov/science-and-technology/csd-ddosd
[18] CSD. Process control systems security. https://www.dhs.gov/science-and-technology/csd-pcs
[19] CSD. Linking the oil and gas industry to improve cyber security (LOGIIC). https://www.dhs.gov/science-and-technology/csd-logiic
[20] CSD. Trustworthy cyber infrastructure for the power grid (TCIPG). https://www.dhs.gov/science-and-technology/csd-tcipg
[21] Automation Federation. LOGIIC. https://www.automationfederation.org/Logiic/logiic
[22] Automation Federation. Cyber security implications of SIS integration with control networks. http://www.automationfederation.org/filestore/af/logiic/LOGIIC SIS REPORT for ISA August 25 2011 mod jan 2013.pdf
[23] Automation Federation. Cyber security implications of SIS integration with control networks. The LOGIIC SIS Project. https://logiic.automationfederation.org/public/

Shared Documents/LOGIIC SIS AW11 Final PPT. pdf
[24] Automation Federation. LOGIIC HPS final project report. http://www. automationfederation. org/filestore/af/logiic/LOGIIC Project 3 AWL Report. pdf
[25] Automation Federation. LOGIIC wireless project final public report. http://www. automationfederation. org/filestore/af/logiic/Project_5_Public_Report_Final. pdf
[26] Automation Federation. A. McIntyre. LOGIIC virtualization project final public report. 2015. http://www. automationfederation. org/Content/Documents/P8PublicReport. pdf
[27] Automation Federation. A. McIntyre. LOGIIC remote monitoring project public report. 2015. http://www. automationfederation. org/Content/Documents/P7PublicReport. pdf
[28] CSD. Moving target defense. https://www. dhs. gov/science-and-technology/csd-mtd
[29] 唐秀存，许强，大伟，徐良华. 移动目标防御(MTD)关键技术研究. 微型机与应用. 2016，(07)
[30] DETER. DETER project history. http://www. deter-project. org/deter_history
[31] Alefiya Hussain，Saurabh Amin. NCS security experimentation using DETER. http://www. Truststc. org/pubs/904/hicons12_submission_13. pdf
[32] USENIX. Very large scale cooperative experiments in emulab-derived systems. https://www. usenix. org/legacy/event/deter07/tech/full _ papers/sklower/sklower _ html/
[33] DHS. NIPP 2013 partnering for critical infrastructure security and resilience. https://www. dhs. gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508. pdf
[34] DHS. NIPP security and resilience challenge 2016 overview fact sheet. https://www. dhs. gov/sites/default/files/publications/nipp-challenge-submissions-fact-sheet-06-16-16-508. pdf
[35] DHS. The next generation cyber infrastructure (NGCI) Apex program. https://www. dhs. gov/science-and-technology/apex-ngci
[36] DHS. Next generation cyber infrastructure Apex fact sheet. https://www. dhs. gov/publication/next-generation-cyber-infrastructure

第 3 章　美国能源部

1977 年，美国联邦政府整合了分散在 40 多个联邦机关的能源管辖机构，成立了能源部（Department of Energy，DOE）。《能源部组织法》于 1977 年以较少争议情况下在国会获得通过。美国能源部成立之后，负责制定有效能源政策和管理能源事务，具体包括实施协调统一的国家能源政策、建立统一的节能战略、开发新兴再生能源，确保成本合理和充足可靠的能源供应等。

图 3-1 给出了能源部 2016 年组织结构，目前能源部设有：核安全和国家和安全管理办公室、科技和能源办公室、管理和绩效办公室及直属部长管辖的办公室及其他机构。能源部还设置了能源部长咨询、政策、能源、信贷审查、核安全等一系列委员会，其分工明确，相互独立，以辅助能源部在能源领域制定较为全面

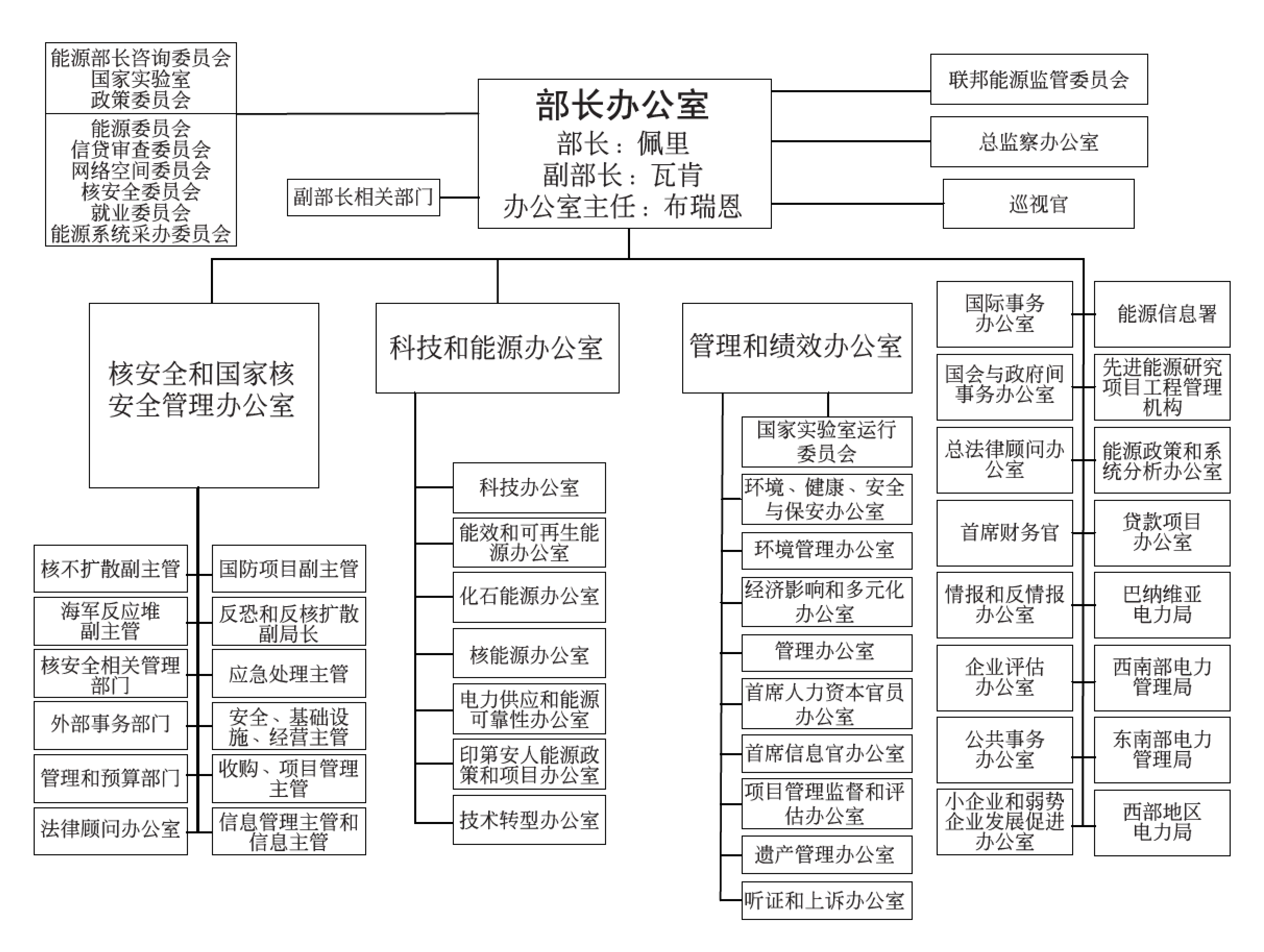


图 3-1　美国能源部组织结构图

和高效的政策和战略。此外，能源部还设立了联邦能源监管委员会、总监察办公室和巡视官，主要实施其对行政管理、项目实施监督监察的职责。能源部的部门架构也在根据国家能源需求和国内国际能源形势不断做出调整。

3.1 美国能源部国家实验室基本情况

国家实验室是国家最高技术水平的代表，其核心使命就是满足国家战略需求，瞄准国家的战略发展目标和世界科技前沿方向，在科技领域开展重大技术攻关和前沿基础研究工作。

如图 3-2 所示，美国的 17 个国家实验室由美国能源部的三个办公室管理。其中，科学办公室管理 10 个，能源办公室管理 4 个，核安全办公室管理 3 个。17 个实验室中，只有国家能源技术实验室是能源部单独管理和运营的。其余 16 个都是以“政府所有-合同制管理”的方式来进行运营的，这 16 个实验室的实际运营者包括大学、公司和联合组织等法人单位。这些实验室的具体管理方式如表 3-1 所示。

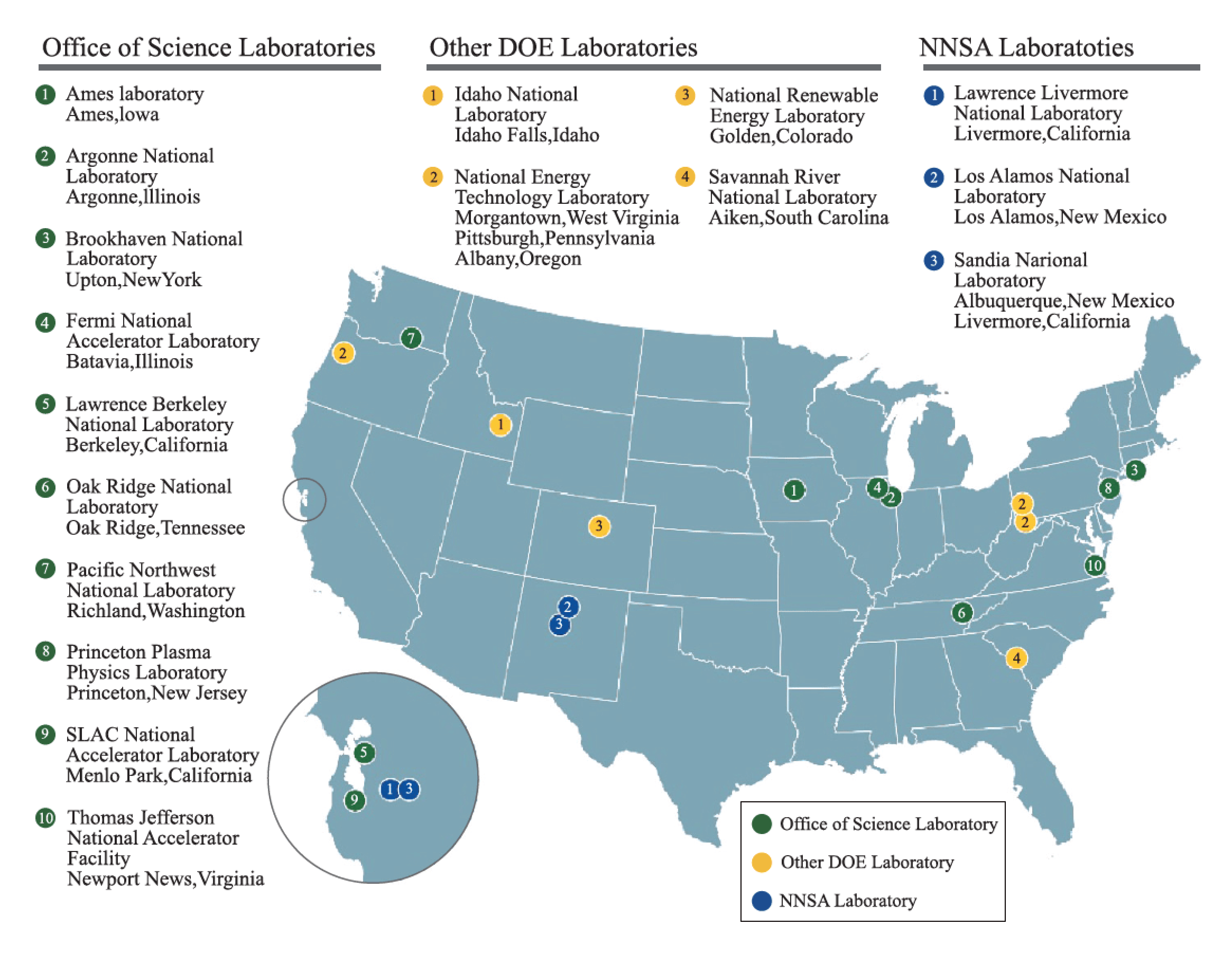


图 3-2 美国能源部 17 个国家实验室地理分布图[1]

表 3-1　美国能源部 17 个国家实验室管理方式一览表

编号	实验室名称	能源部管理部门	运营者
1	艾莫斯实验室 Ames Laboratory	科学办公室	爱荷华州立大学 Iowa State University
2	阿贡国家实验室 Argonne National Laboratory	科学办公室	芝加哥大学 University of Chicago
3	劳伦斯伯克利国家实验室 Lawrence Berkeley National Laboratory	科学办公室	加利福尼亚大学 University of California
4	普林斯顿等离子物理实验室 Princeton Plasma Physics Laboratory	科学办公室	普林斯顿大学 Princeton University
5	斯坦福直线加速器中心 Stanford Linear Accelerator Center	科学办公室	斯坦福大学 Stanford University
6	费米国家加速器实验室 Fermi National Accelerator Laboratory	科学办公室	Fermi Research Alliance LLC 费米研究联盟责任有限公司
7	橡树岭国家实验室 Oak Ridge National Laboratory	科学办公室	田纳西大学与巴特尔纪念研究所 University of Tennessee and Battelle Memorial Institute
8	托马斯杰斐逊国家加速器装置 Thomas Jefferson National Accelerator Facility	科学办公室	杰斐逊科学协会 Jefferson Science Associates
9	布鲁克海文国家实验室 Brookhaven National Laboratory	科学办公室	布鲁克海文科学协会 Brookhaven Science Associates
10	西北太平洋国家实验室 Pacific Northwest National Laboratory	科学办公室	巴特尔纪念研究所 Battelle Memorial Institute
11	劳伦斯利弗莫国家实验室 Lawrence Livermore National Laboratory	核安全办公室	劳伦斯利弗莫国家安全责任有限公司 Lawrence Livermore National Security LLC

续表

编号	实验室名称	能源部管理部门	运营者
12	洛斯阿拉莫斯国家实验室 Los Alamos National Laboratory	核安全办公室	洛斯阿拉莫斯国家安全责任有限公司 Los Alamos National Security LLC
13	桑迪亚国家实验室 Sandia National Laboratory	核安全办公室	桑迪亚公司 Sandia Corporation
14	国家可再生能源实验室 National Renewable Energy Laboratory	能源办公室	可持续能源联盟责任有限公司 Alliance for Sustainable Energy LLC
15	爱达荷国家实验室 Idaho National Laboratory	能源办公室	伯特立能源联盟 Battelle Energy Alliance
16	萨瓦纳河国家实验室 Savannah River National Laboratory	能源办公室	萨瓦纳河核能解决方案责任有限公司 Savannah River Nuclear Solutions LLC
17	国家能源技术实验室 National Energy Technology Laboratory	能源办公室	能源部 Department of Energy

能源部的电力调度与能源可靠性办公室(Department of Energy's Office of Electricity delivery & energy reliability,DOE-OE)也是能源部内部一个非常重要的办公室。该办公室负责管理着能源部在工业控制系统安全方面最为著名的国家SCADA测试床(National SCADA Test Bed,NSTB)项目[2]。能源部管辖着7个国家实验室(橡树岭、西北太平洋、洛斯阿拉莫斯、爱达荷、阿贡、桑迪亚、劳伦斯伯克利国家实验室)是NSTB项目的主要参与单位。NSTB项目组织架构如图3-3所示。

接下来,3.2节介绍美国能源部针对能源行业控制系统的安全防护所制定的安全防护技术路线。3.3节介绍国家SCADA测试床NSTB平台的总体情况,并以NSTB作为主线,分别介绍了相关国家实验室的各自内容和在NSTB项目中的工作情况。

3.2 能源行业控制系统安全防护技术路线

能源行业工业控制系统是支撑电力、煤炭、天然气、石油石化等一系列与能源生产调度相关的控制系统,是国家关键基础设施的重要组成部分,而目前伊

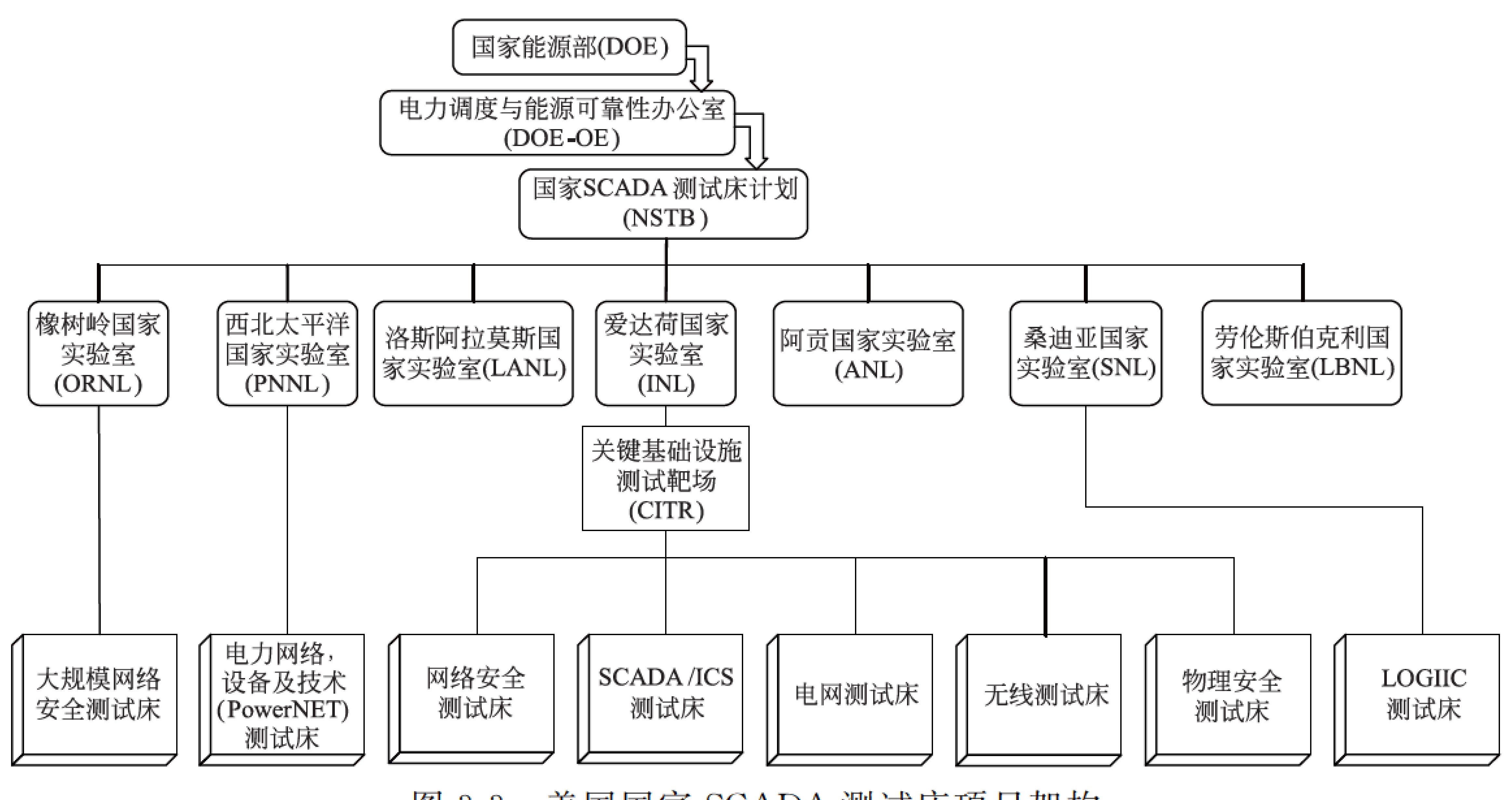


图 3-3　美国国家 SCADA 测试床项目架构

朗、乌克兰等国频频发生的电力、核设施工控网络安全事件不断地警醒着世人，能源设施的网络安全防护能力已直接关系到国家的能源安全问题，必须重视建设与能源设施配套的安全防御机制和技术，才能保证国家能源安全。

美国能源部为了加强能源行业的系统安全防护水平，分别于 2006 年和 2011 年发布了两份关于能源行业控制系统安全的规划文档[3,4]。这两份文档都以 10 年为一个总的时间周期，按照短期(0～3 年)、中期(4～7 年)和长期(8～10 年)三种目标分别对能源行业的控制系统安全防护做出了具体的发展规划和要求。

3.2.1　2006 年技术路线

2006 年技术路线的总体目标：到 2015 年，能源行业控制系统在工作周期中的各个环节(设计、安装、运营和维护)，都具备抵抗恶意攻击的能力，并且配套的软硬件防护手段不会影响关键系统的功能。

2006 年技术路线中，能源部制定了四个战略方向：

(1) 明确安全态势：企业应该彻底地摸清他们目前的安全态势，以此来找出系统脆弱点，并采取相应的措施来消除安全隐患。能源部将帮助能源设施运营者们，提高其自动化安全态势感知的能力和发生故障事件后的及时自我修复能力。

(2) 研发可靠的安全防护技术：当识别出安全风险以后，企业和能源部应提出相应的解决方案来降低系统风险。此外，通过整合安全防护技术，在下一代控制系统的架构和组件中应该能提供一种内生的端到端安全服务。

(3) 研发入侵检测技术和制定应急响应策略：能源行业的控制网络应逐步具有入侵检测和应急响应能力。

(4) 保持安全改进：能源设施运营者、管理者和政府应齐心协力地来不断加强安全防护措施。

同时，能源部在该文档[3]中还针对这四个战略方向列举了具体的工作：

(1) 建立一个美国政府国家级安全事件和信息共享环境和平台；制定一个大家普遍认同的用于测定安全态势的清晰准确度量标准；研发一个用于模拟网络攻击和响应的仿真工具。

(2) 研究适用于 SCADA 控制网络与企业网络连接的最优方式，提高陈旧通信系统中的通信和计算性能，以此来支持加入安全解决方案；研究确立适用于变电站和控制中心之间的网络安全防护实施方案；研发一种不会影响控制系统 7×24 全天候运行的补丁修复方案，并为控制系统研发一种更具鲁棒性的操作系统；研发即插即用的安全模块和经济实用的网关设备，该类模块和设备包含防火墙、入侵检测和抗病毒的功能，并且要尽可能减少对主机运行的影响。

(3) 研发包括安全事件报告和可视化展示的自动化安全事件信息数据收集工具；制定一套确认事故报告原因并提供解决方案的流程规范，提高信息共享和事故报告工作效率；提供安全事件响应培训课程、技术和工具，研发入侵检测和防御系统来为网络和主机提供更加鲁棒的应用。

(4) 研发安全数据交互和通信的标准规范，提供信息安全培训课程；建立与学校合作的项目来促进关于控制系统安全的教学工作；通过立法或其他鼓励机制，加快建立信息共享机制，以此来持续不断地加强和改进能源行业关键基础设施安全防护技术。

3.2.2 2011 年技术路线

2011 年总体目标：到 2020 年，实现“能源传输弹性系统”(resilient energy delivery systems)，完成系统设计、部署、运营、维护等一系列的工作，形成能够抵抗网络安全攻击且能够在被攻击情况下维持能源行业控制系统关键功能的能力。

能源部在 2006 版技术路线方向上做了一些改进和补充，重新制定了五个战略方向：培养安全文化和意识，提高风险评估和监控能力，研发新型保护措施，正确处理安全事件的机制，持续保持安全改进。与 2006 版技术路线相比，2011 版[4]增加了培养安全文化与意识的要求，并将之前的研发入侵检测技术和应急响应策略提升为正确处理安全事件机制。同时，能源部也针对这五个战略方向列举了具体的工作：

(1) 培养安全文化与意识：研发一个可供设备供应商和拥有者们进行脆弱

性评估的工具;建立实现一个系统脆弱性和补丁修复管理培训项目,并制定相关政策;开展工业控制系统相关专业认证工作。

(2) 提高风险评估和监控能力:针对能源输送系统,制定一套安全威胁场景和对应的安全风险评估指标,确定安全态势的描述特征;根据当前缓解网络风险水平的需求来标定能源输送系统的安全等级;研发一套风险评估工具,用以评估系统脆弱性、制定风险控制优先策略和设计安全代价估算方法;开发实时安全状态监测可视化工具,以此来标定系统的安全基准状态;提出能源输送系统安全基准,并在部署新解决方案后观测比较安全态势的变化。

(3) 研发新型保护措施:分别开发适用于静态和动态的代码自动化审查工具;开发一种支持动态裁剪可定制化的安全防护机制,为所有系统和设备的授权和管理工作提供按需安全服务;为应用程序和通信设备制定白名单功能;为通信链路研发可信平台模块和可信网络;开发者和运营者共同实现一个包括搭建、集成和运营全过程的安全弹性能源输送系统。

(4) 正确处理安全事件:针对安全事件的网络或物理影响,开发一种能够衡量系统弹性程度的方法和衡量标准;开发实时攻击检测、修复和恢复工具来应对网络安全事件;提高在安全事件响应和恢复的过程中遏制安全攻击的能力;通过建立安全边界划分来研发一种能够控制和阻止入侵攻击的能力。

(5) 持续保持安全改进:建立一个全球性的具有隐私保护功能的信息共享门户(如漏洞发布平台或论坛);建立一个公认的控制系统脆弱性报道发布的流程;完善政府鼓励研发机制,激励企事业单位、学校等科研机构对关键基础设施安全防护研发工作的持续投入。

3.3　国家 SCADA 测试床 NSTB

国家 SCADA 测试床项目(National SCADA Test Bed,NSTB)[2],由能源部的电力调度与能源可靠性办公室(Department of Energy's Office of Electricity delivery & energy reliability,DOE-OE)负责,通过结合国家实验室拥有的先进硬件设备和相关专业人员的研究、开发、分析能力,发现和解决 SCADA 系统的关键安全问题,应对能源行业所面临的安全威胁,减少网络攻击给能源控制系统所带来的破坏。

NSTB 项目由 DOE-OE 创建。DOE-OE 是能源部负责创建更加现代化的、有弹性的、安全的电力传输基础设施的最主要的办公室。DOE-OE 的主要目标就是:促进、主导和管理国家在电网现代化建设,能源基础设施安全防护,能源系

统从安全事件或故障中恢复等方面的研发投入，以此来满足美国对可靠、高效、弹性能源基础设施的需求。为了实现该目标，并且减少由于网络攻击给能源控制系统所带来的破坏，DOE-OE 在 2003 年创建了 NSTB 项目。NSTB 项目旨在提高控制系统的安全，并且保护能源行业基础设施和能源设施所服务的其他行业设施。NSTB 项目与能源行业控制系统安全防护技术路线、美国国家政策、联邦政府角色、DOE-OE 目标、NSTB 设施和资源及其他相关部门的目标是相辅相成的。并且，NSTB 项目对于实现 DOE-OE 的目标发挥着至关重要的作用。

NSTB 项目与国家实验室紧密相关。美国能源部目前管辖着的 17 个国家实验室大多数是核领域的知名实验室。随着近年来国家对工业控制系统安全越来越重视，其中多个实验室的研究内容也都逐渐与工业控制安全相关。这些实验室也在工业控制安全及关键基础设施安全方面投入了大量的人力、物力、财力，并开展了一系列研发项目。其中，NSTB 项目汇集了阿贡、爱达荷、劳伦斯伯克利、洛斯阿拉莫斯、橡树岭、西北太平洋和桑迪亚国家实验室的专家和专业人士，搭建了一个国家级 SCADA 测试床。

3.3.1 NSTB 研究内容

如图 3-4 所示，NSTB 项目的实施需要依据能源部控制系统安全技术路线，

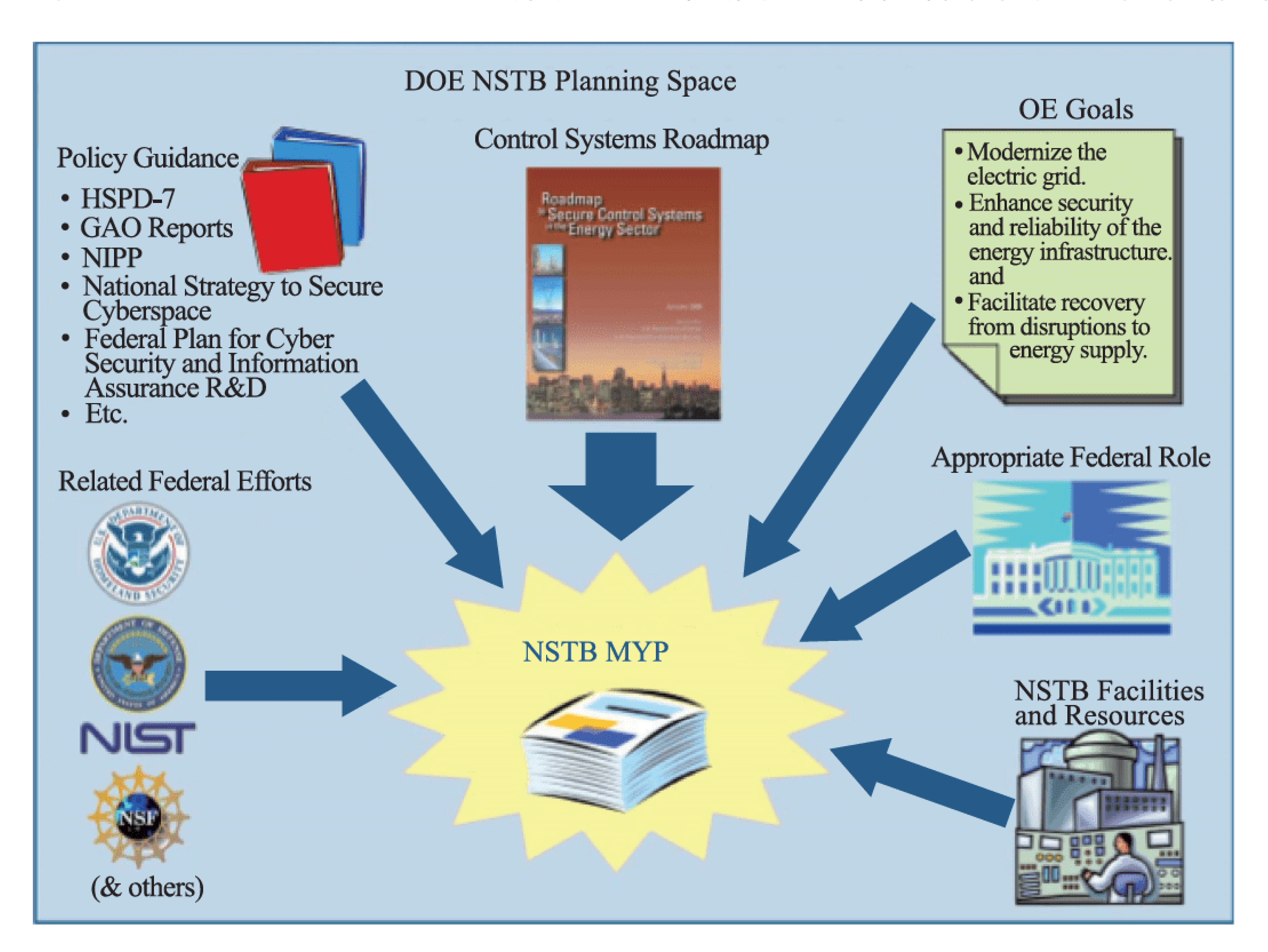


图 3-4　NSTB 计划涉及的范围（来源：文献[6] Exhibit 2.2 DOE NSTB Planning Space）

DOE-OE 目标等多项国家级政策和方针，结合 NSTB 项目涉及的设施和资源，在联邦政府及相关部门的配合和支持下来完成既定的任务和目标。NSTB 项目的主要任务[5]包含四个方面：

(1) 提高工业控制系统对网络安全漏洞问题的认知能力，识别、评估和解决当前的 SCADA 系统漏洞；

(2) 针对现有控制系统的安全问题，通过测试床测试研究并开发出短期应对方案和风险缓解策略；

(3) 设计下一代工业控制系统安全架构，建设智能、安全、可靠的控制系统和基础设施系统；

(4) 研究制定国家标准和指导方针。

如图 3-5 所示，为了实现 NSTB 上述四方面的主要任务，NSTB 重点研究以下三个内容[6]：

(1) 系统脆弱性评估：对电力、石油和天然气等关键行业的控制系统进行安全评估，促进新一代控制系统的研发工作；鼓励能源行业厂商和运营者及时修复安全漏洞，制定下一代的系统设计和实施规范。

(2) 综合风险分析：通过了解现有的网络安全态势来确定能源行业控制系统的安全风险，制定解决方案；开发一套端到端、网络威胁和漏洞分析工具。

(3) 研发新一代控制系统：加强下一代控制系统的内生安全性，专注于设计创新体系结构，研发新型控制系统安全组件和安全通信技术。

3.3.2 NSTB 项目实验室分工

在 NSTB 项目研发中，各实验室的基本分工[2]如下(参与项目的实验室如图 3-6 所示)：

(1) 爱达荷国家实验室(INL)

研发一个在能源行业通用的网络安全威胁信息分析工具，帮助能源行业的运营者分析并理解这些安全威胁是如何影响整个风险态势走向的。该工具允许运营者应对一个特定的安全威胁给予适当的反馈。此外，爱达荷实验室还负责了关键基础设施测试靶场的建设工作，搭建了网络安全测试床、SCADA/ICS 测试床、电网测试床、无线测试床和物理安全测试床。

(2) 桑迪亚国家实验室(SNL)

研究移动目标防御技术，具体包括 IP 地址可变、通道数可变、路由和 IPSec 信道可变、执行代码随机、指令集合随机等。通过在网络配置方面和设备部署方面增强信息不确定性、动态变化性等方式来增加攻击者进行系统分析和攻击的

OE Goal

To lead national efforts to modernize the electric grid,enhance the security and reliability of the energy infrastructure,and facilitate recovery from disruptions to the energy supply.

NSTB Program Goal

Reduce the risk of energy disruptions due to cyber attack on control systems

Challenges

- Increasingly sophisticated abversary capabilities
- Complexity increases with each interconnection
- Security fixes for legacy systems may dagrade performance
- Integration of next generation technology into legacy control systems
- Lack of secure methods for information sharing
- Limited ability to measure and assess control sysetem risk
- Poor understanding of cyber threats and consequences
- Weak business case for cyber security investments
- Adoption of smart technologies may increase vulnerabilities

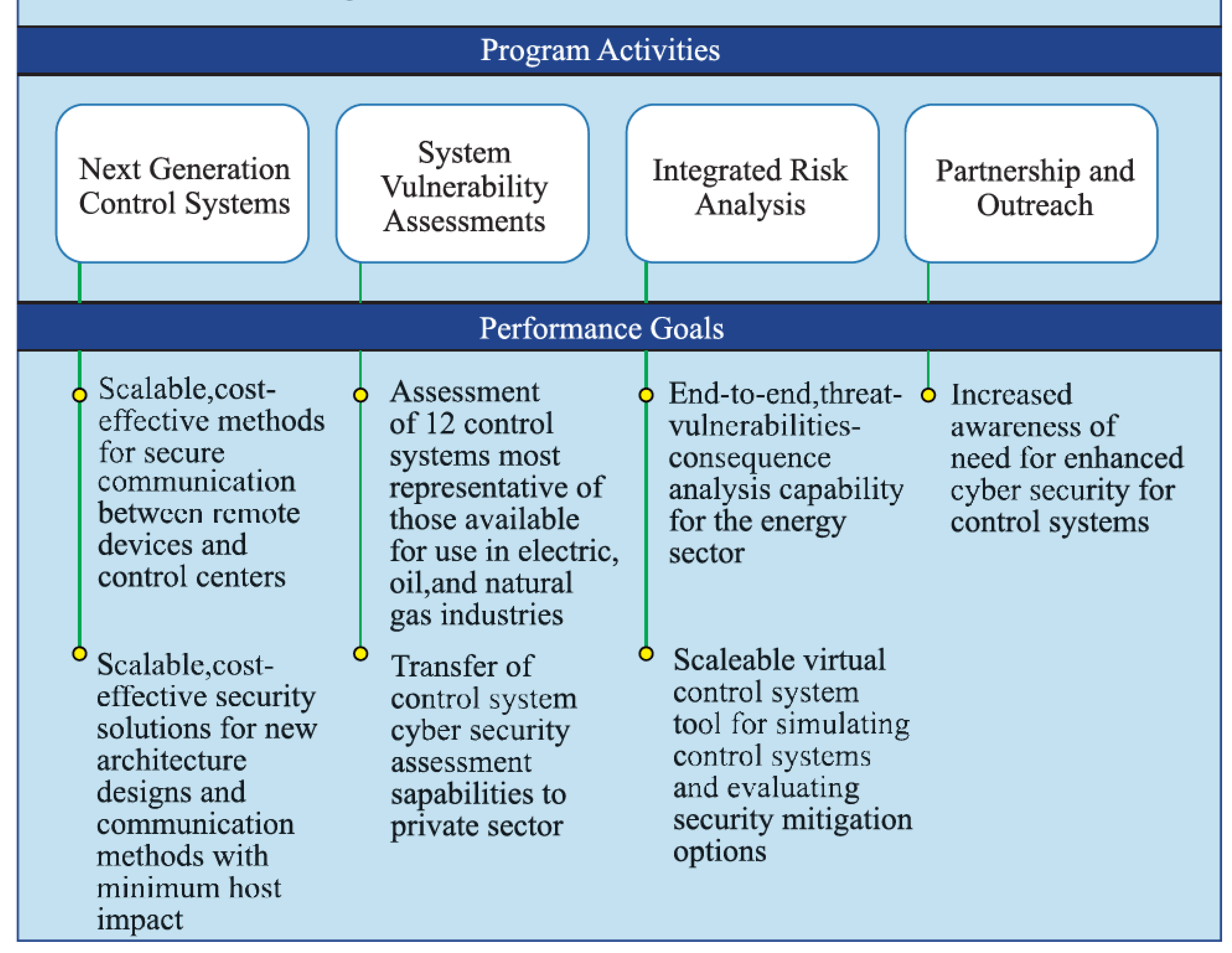


图 3-5　NSTB 项目架构图(来源：文献[6] Exhibit 2.3 Strategic Framework for NSTB Program)

难度，降低系统脆弱性。此外，实验室还开展了油气工业网络安全研究，以美国桑迪亚国家实验室为首、14 个机构参与的为期一年的 LOGIIC 已告结束，并将继续开展实地测试。

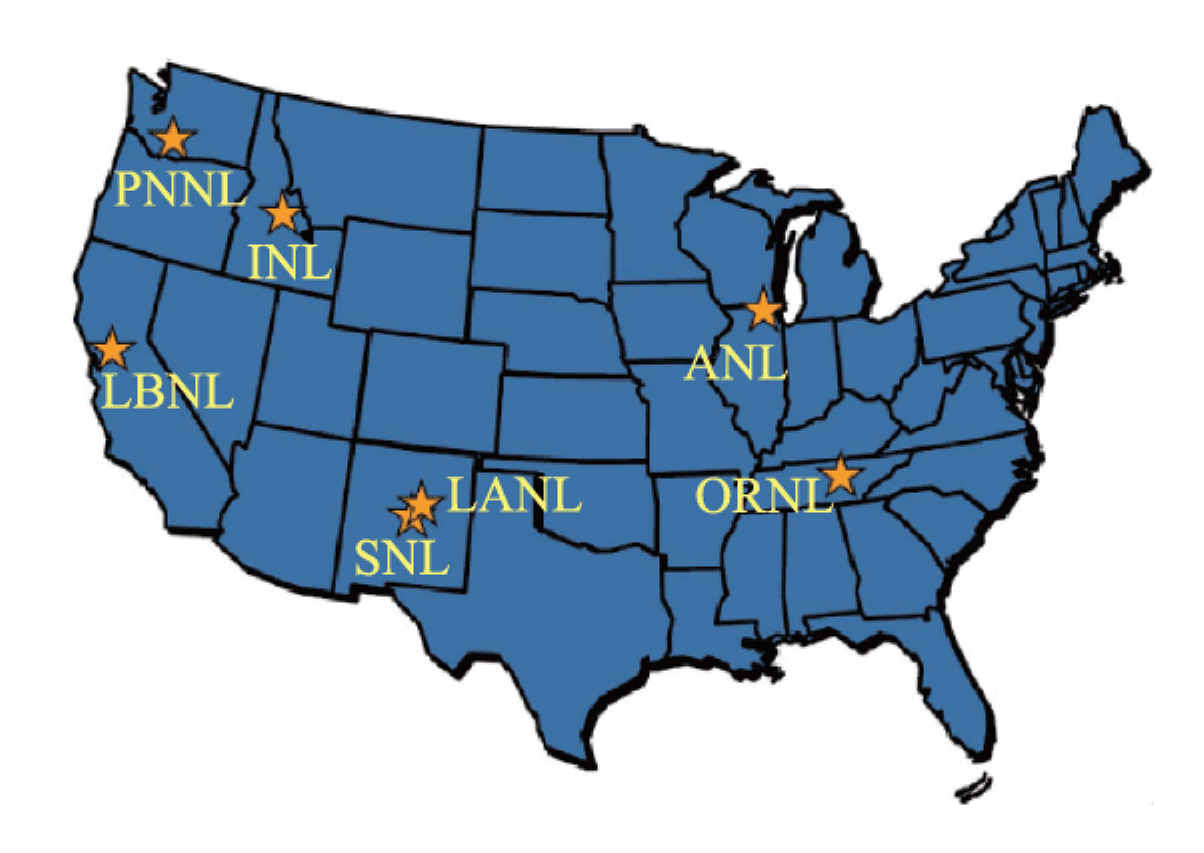


图 3-6　NSTB 项目参与实验室

(3) 洛斯阿拉莫斯国家实验室(LANL)

负责在能源系统(如电网系统)中,研究量子密钥分发机制,得到可应用于传统加密认证算法中的密钥。

(4) 阿贡国家实验室(ANL)

通过国家标准化协会国际联盟(International Federation of the National Standardizing Associations, ISA)工作组来制定包括国际电工委员会(International Electrotechnical Commission,IEC)61850 变电站自动化和可信赖的无线工控标准等控制系统标准。此外,阿贡实验室还利用其在石油和天然气行业的专家来为建设 NSTB 做贡献。

(5) 西北太平洋国家实验室(PNNL)

研究能源行业安全 SCADA 通信协议(Secure SCADA Communication Protocol,SSCP)、开发现场设备管理软件、开发加密信任管理软件、开发协议分析器等组成一整套开源工具,以此识别出调试前和调试期间能源输送系统中被攻击的软、硬件。该套件包括一系列独立的工具,它可以在本地运行来保证硬件供应链安全,也可以在关键基础设施的供应链中开展大规模高性能计算服务,分析系统运行状况并识别出潜在的问题。此外,实验室还搭建了电力网络、设备及技术测试床 PowerNET。

(6) 橡树岭国家实验室(ORNL)

研究适用于能源行业系统的量子密钥分发机制。旨在通过改进传统的量子密钥分发机制来进一步降低开销。该实验室所研发的新型量子密钥分发机制允许多个客户端通过一个量子通信信道使用低成本的量子调节器来实现密钥分发。此外,实验室还搭建了大规模网络安全测试床。

(7) 劳伦斯伯克利国家实验室(LBNL)

基于传感器或执行器的物理资源限制条件,研究系统运行状态监测机制。

当存在来自系统外部或内部安全威胁时，该机制旨在监测系统运行状态或流程有悖于既定协议的异常情况。此外，该项目还会研究相对应的安全防御和保护机制。

3.3.3 NSTB 实验室具体情况

3.3.3.1 爱达荷国家实验室

如图 3-7 所示，在 NSTB 项目中，爱达荷国家实验室（INL）关键基础设施测试靶场[7,8]发挥着举足轻重的作用。靶场旨在使用与现实生产中完全相同的设备来构建一种全实物的大型测试床，完全复制真实系统，研发保护国家基础设施的技术，并开展大量的测试和验证工作。在基础设施建设方面，为保证各实验床能够高效运作，INL 在基础设施建设方面已经投入超过 1 亿美元。目前，该项目所拥有的基础设施包括：安全的配电系统（3 个发电厂、7 个变电站，共计 61 公里的 138kV 电力线路），隔离部分电网/变电站的设备，电力线路试验区，集中式 SCADA 操作中心，无线网络，以太网，下一代蜂窝网络，无线频谱管理设备。该靶场可对国家安全、网络安全、工控安全等多个项目进行研究，如散装或微量爆炸物检测，炸药/武器效应试验，违禁品和武器检测，无线通信、无人机研究与实



图 3-7 INL SCADA 测试床（来源：文献[7]）

验，工控网络安全和物理安全实验。

目前，该测试靶场已经具备了以下科研基础。

(1) “清洁”频谱：远离城市地区或军事基地，实现本地频谱管理，可以使用下一代/国际频率。

(2) 各种大规模通信网络：全球移动通信系统（Global System for Mobile Communication, GSM），通用移动通信系统（Universal Mobile Telecommunications System, UMTS），固定全球微波互联接入（Worldwide Interoperability for Microwave Access, WiMAX），移动 WiMAX，码分多址（Code Division Multiple Access, CDMA），高频、微波网络等实验网络。

(3) 灵活的多资源实验能力：拥有 SCADA 系统、物理和网络设备等多种基础设施资源，具有研发、集成、独立验证与测试等综合实验能力。

1. 实验室研究目标

INL 作为美国能源领域的领头单位，致力于在能源、国家安全和生态环境方面为能源部研究制定战略目标，并力争在保证关键基础设施安全的前提下，改变世界能源的未来。在工控安全方面，INL 旨在通过研发、示范和推广项目来确保国家能源安全。具体地，INL 将努力提高国家在工业网络安全威胁分析，无线通信频谱利用率，电网可靠度、安全性和恢复性等方面的研发能力，以此来实现物理和网络安全的一体化。

2. 实验室研究内容

INL 主要研究工业控制系统网络安全、关键基础设施保护、关键系统漏洞分析、信息物理系统保护、仪器控制和弹性控制系统等内容，开展工业控制系统和信息物理系统的安全保护研究。

3. 爱达荷实验室建设运营的测试床

INL 运营着 5 个国家测试床，分别是网络安全测试床、SCADA/ICS 测试床、电网测试床、无线测试床、物理安全测试床。

(1) INL SCADA 测试床

INL 的基础设施测试床将大规模部署的 SCADA 组件与由行业提供并在实验室内安装的系统相结合。可以对多个 SCADA 和过程控制系统在实验室中进行实时地设计，开发，集成，系统化及应用示范。控制系统和网络专家检查系统的组成部分，寻找系统组件固有的脆弱性。行业和政府客户可以把它们的远程

终端单元、智能电子设备和可编程逻辑控制器置于测试床中，并开展进一步的测试和开发。

(2) INL 电网测试床

图 3-8 给出了 INL 电网测试床的实物图。该测试床开发了一套建模与仿真工具，以研究新技术对电网可能产生的影响，模拟实时动态电网网络，检测未知漏洞，提供电网故障应对策略。在这套工具的顶端是实时数字仿真器(Real Time Digital Simulator，RTDS)，该仿真器是一个全数字化电磁瞬态电力系统仿真器，支持实时操作。此外，测试床中的高压交流电(High Voltage Alternating Current，HVAC)和高压直流电(High Voltage Direct Current，HVDC)提供了电力系统真实仿真验证环境。





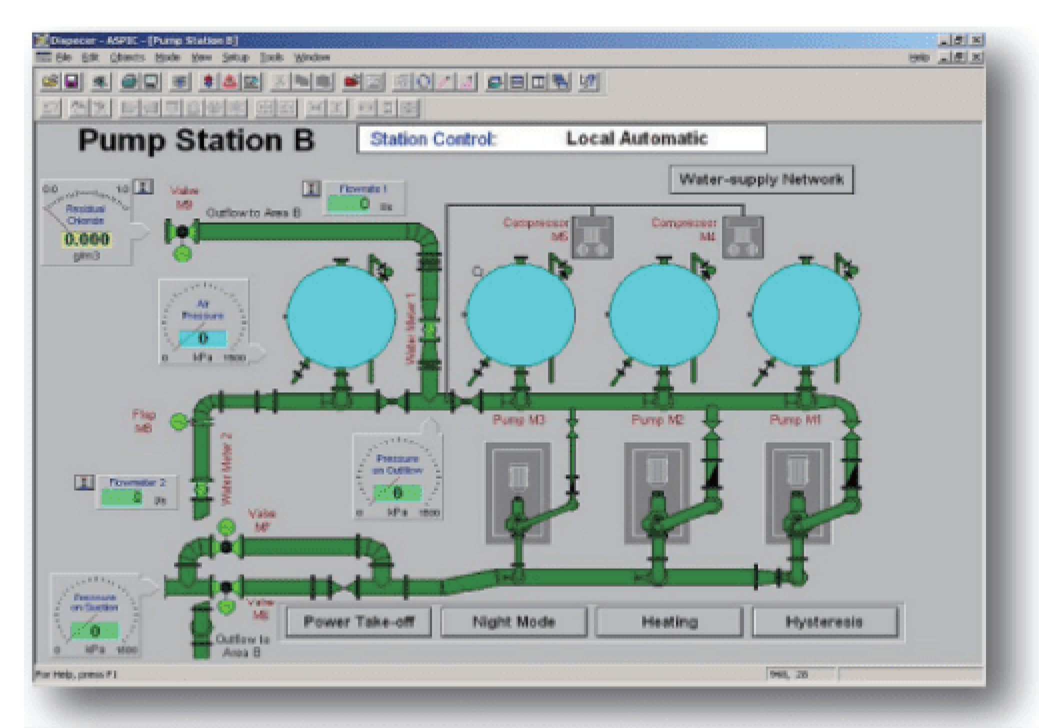
图 3-8　INL 电网测试床(来源：文献[7])

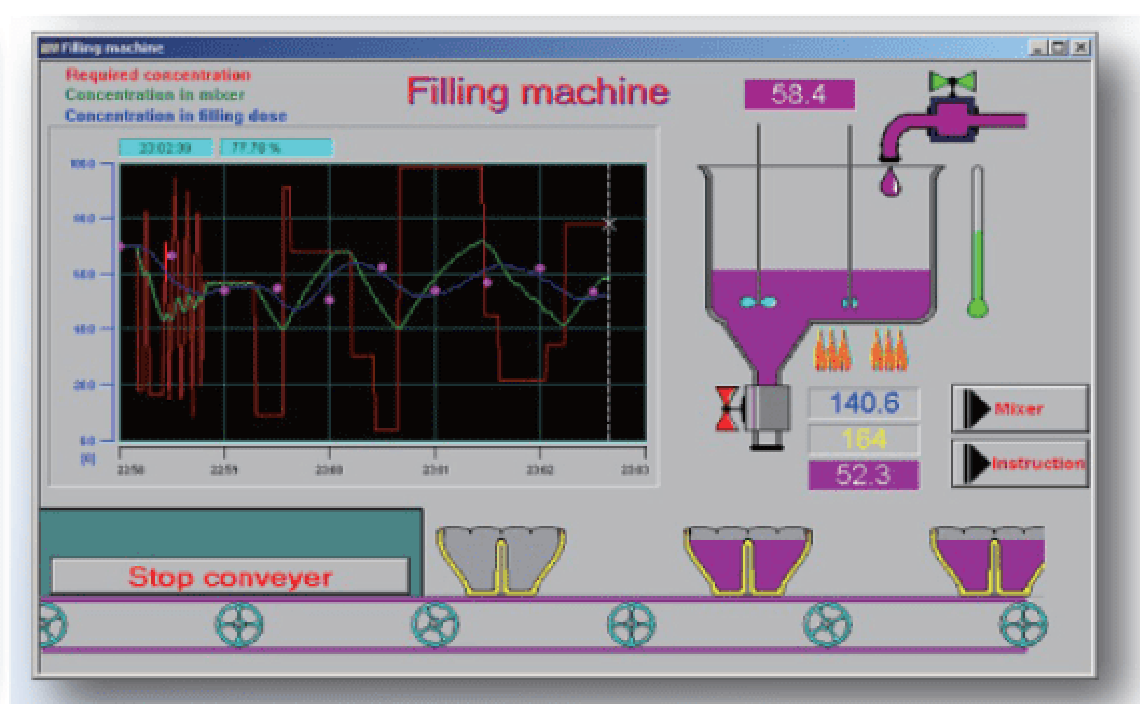
(3) INL 网络安全测试床

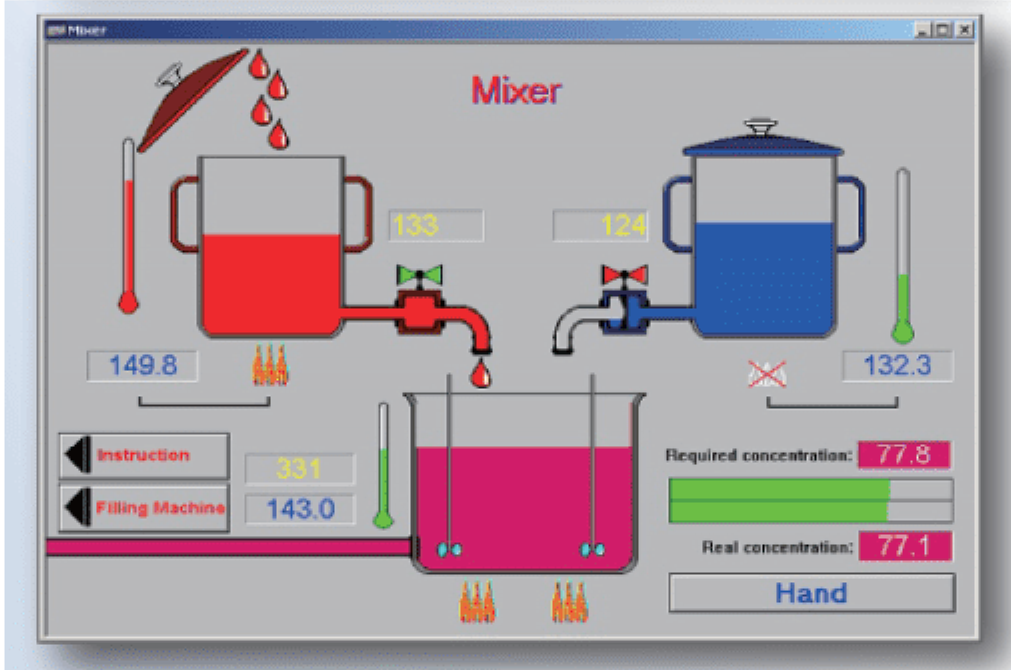
图 3-9 给出了 INL 网络安全测试床的实物图。该测试床支持让用户访问多个机密和非机密的试验设施和关键基础设施测试靶场的组件，研究人员能够提供一个定制的无线通信入侵检测系统，对漏洞进行评估分析。利用该测试床，研究人员还可以灵活地根据客户需求来修改攻击测试规范，以此来攻击系统，进而对系统的脆弱性进行有针对性的评估和检测。利用全实物测试床技术，该测试床能对控制系统进行精确复制，可以进行大规模网络攻击测试。网络安全研究人员通过利用网络恐怖主义和黑客的方法和意识形态，可对网络进行模拟攻击，由此找出网络系统的脆弱性所在，并通过分析评估，提出防御方案。测试床还有利于开发漏洞修复技术和工具，帮助国家重要基础设施发现并减少网络漏洞。

(4) INL 无线测试床

该测试床拥有 2300 平方公里的无线测试范围，提供一个无线射频(Radio







INL's Cyber Security Test Bed has the flexibility to replicate any customer's control system specifications.

图 3-9　INL 网络安全测试床(来源:文献[7])

Freqency, RF)实验环境,尽量减少来自农村/城市,机场或军事因素的干扰,支持研究人员用于从事无线网络的研究、开发、集成、测试和演示工作。研究人员已完成了无线网络检测及手机、传感器和应用程序的集成检测,可进行全国范围内的远程无线连接研究和实验。实验室与企业合作,在 GSM,UMTS,WiMAX,CDMA,高频,微波,Wi-Fi 和甚小口径天线地球站终端等方面,提供了专业的技术支持。此外,在无人机领域,实验室已为 50 多个行业领先的软、硬件厂商提供了无线测试服务。

3.3.3.2　桑迪亚国家实验室

1. 实验室研究目标

桑迪亚国家实验室期望解决国家重大能源安全问题,有效提升核威慑能力,并处理好核威慑任务与国家安全任务之间的协同作用和相互依赖关系。为此,实验室制定了四个主要目标:提升核武器威力,提高国家安全影响力,为国家安全建设持续做贡献,制定国家能源战略目标。

2. 实验室研究内容

在核武器方面,与客户、合作伙伴以及桑迪亚实验室的其他研究领域人才一

起协作来提供一个具有物理、信息安全的核威慑力；在保障全球核安全方面，助力美国政府能够自信地参与、评估和解决全球在使用先进系统和技术时所面临的核安全问题；在网络空间防御方面，研发基于科学和工程的网络技术来持续地提升国家安全防御与主导能力；在维持美国国防技术优势方面，研发先进技术和能力来及时应对国家安全和核武器所面临的安全挑战。

3. 桑迪亚国家实验室建设运营的 LOGIIC 测试床[9]

在工业控制系统安全和关键基础设施安全方面，为了保证美国油气控制系统的安全和可靠运行，最大程度减少通过网络攻击损害或瘫痪美国油气基础设施的可能性，实验室在 2004 年就开展了为期一年的 LOGIIC 测试床项目。LOGIIC 测试床项目设计了一种如图 3-10 所示的过程控制系统中的通用信息基础设施理想模型，用来表示精炼厂和油气管网场景的通用信息基础设施系统；分析并确定了系统所有可能被攻击者利用的脆弱环节和可能存在的攻击场景；设计了一套模拟测试床，通过假设攻击情景来评估油气工业的潜在威胁。在过程控制系统中，研究了网络安全攻击所导致的系统异常行为；研究了安全事件之间的关联关系，以此来加强入侵检测能力；设计了一个通过部署安全传感器来监测系

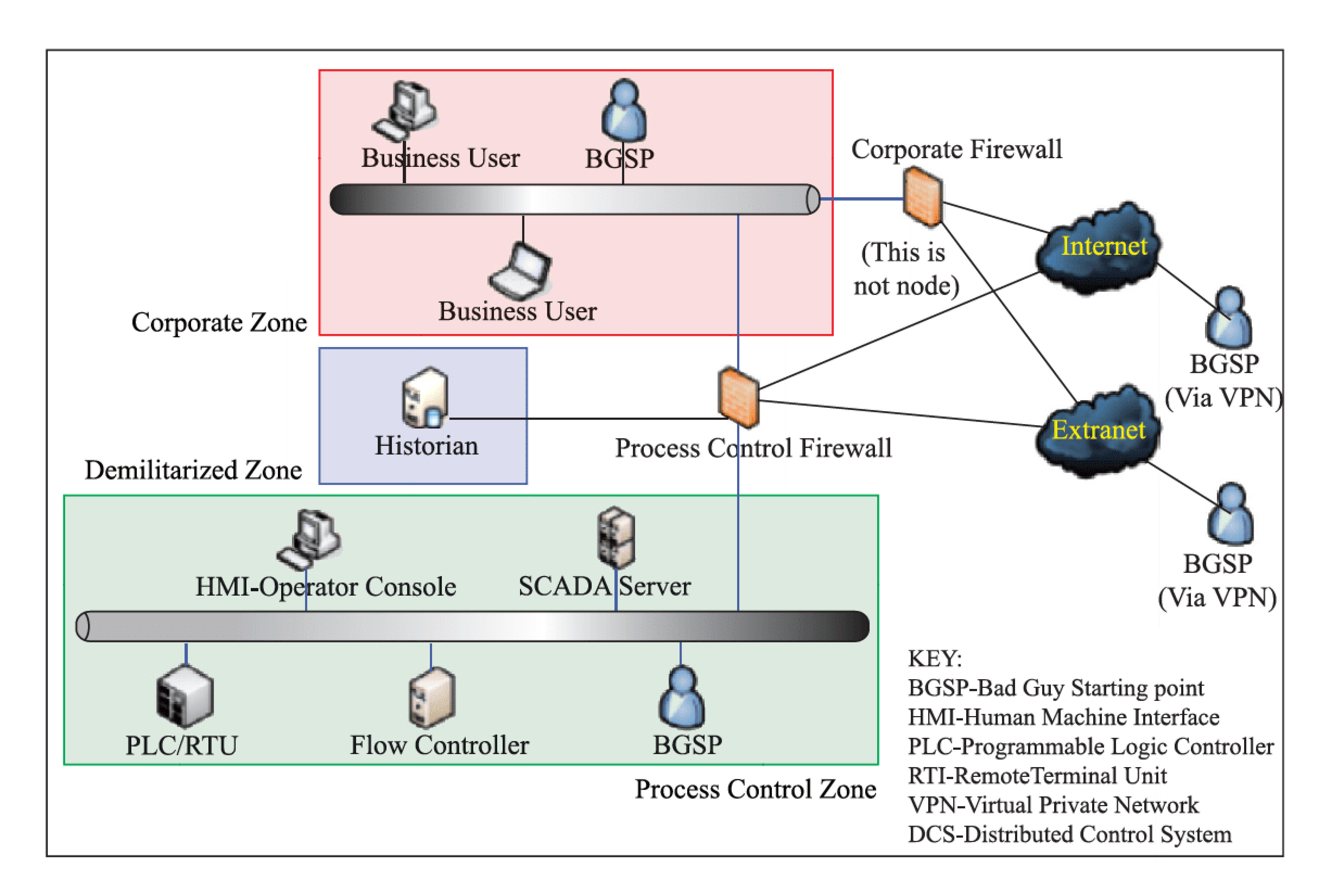


图 3-10 过程控制系统中的通用信息基础设施的理想化模型（来源：文献[9] Figure 2）

统运行状态的纵深防御体系，以此来监测油气控制系统中的可疑系统状态或行为。

图 3-11 展示了 LOGIIC 项目的测试床环境，这个测试环境模拟的是油气管道和精炼厂的真实环境。测试床包括一个用于管理油气管道的 SCADA 系统，一个用于运行精炼厂的 DCS 系统。

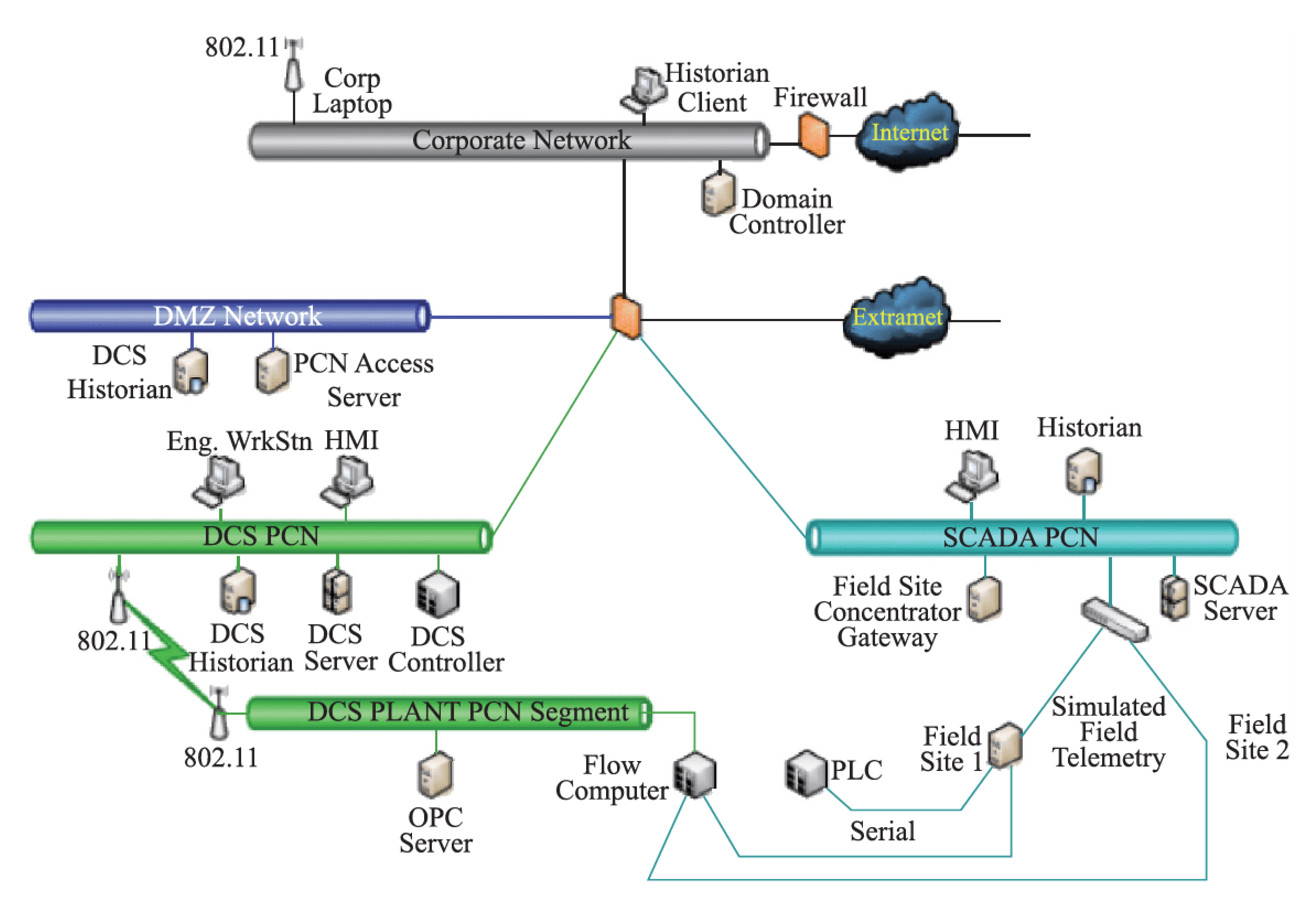


图 3-11　LOGIIC 测试床环境（来源：文献[9] Figure 3）

LOGIIC 系统综合了设备、主机和网络级别的安全事件关联能力，提供了一种设施级别的安全威胁感知方案。LOGIIC 系统支持可扩展性，可包括标准的 IT 防御和控制系统安全定制设备。其中，标准的 IT 防御设备包括：网络防火墙、主机防火墙，网络入侵检测系统，网络设备（有线或无线路由器）。控制系统安全定制设备包括：针对过程控制系统协议的网络入侵检测系统，DCS 和 SCADA 警报系统。

3.3.3.3　西北太平洋国家实验室

1. 实验室研究目标

西北太平洋国家实验室（PNNL）于 1965 年成立，位于华盛顿州的里奇兰（Richland），致力于解决能源、环境和国家安全最棘手的问题。PNNL 支撑国土

802.11
Corp. Laptop
EFW Policy Server
Historian Client
Firewall
Internet
Corporate Network
Domain Controller
IDS
IDS-AV-FM
Extranet
EFW Polioy Server
Correlation System
IDS
DMZ Network
DCS Historian
PCN Access Server
EFW Polioy Server
Eng. WrkStn
HMI
IDS
DCS PCN
802.11
DCS Historian
DCS Server
DCS Controller
IDS
HMI
Historian
EFW Policy Server
SCADA PCN
Field Site Concentrator Gateway
SCADA Server
DCS PLANT PCN Segment
802.11
OPC Server
Flow Computer
PLC
Field Site 1
Simulated Field Telemetry
Field Site 2
Serial

图 3-12　LOGIIC 安全系统架构(来源：文献[9] Figure 4)

安全部、国家核安全局以及其他政府机构的工作，主要研究领域包括环境、卫生、能源、计算机科学与安全。

2. 实验室研究内容

(1) 电网可靠性

西北太平洋国家实验室的电力基础设施运营中心(Electricity Infrastructure Operations Center，EIOC)作为一个独特的电网现代化的新技术研发与部署平



图 3-13　西北太平洋国家实验室电力基础设施运营中心

台，具有实时电网数据的先进计算、分析和可视化能力。EIOC 组建了两个全功能控制室，主要致力于研究电网的可靠性。

（2）安全 SCADA 通信协议

实验室建立了安全 SCADA 通信协议研究项目。研究内容包括构建能源行业安全通信架构、开发现场设备管理软件、开发加密信任管理软件、开发协议分析器。

西北太平洋实验室在 NSTB 项目中，为了研发下一代控制系统，研发生产了包括通用控制系统架构（如图 3-14 所示）、软件、硬件和工具等方面的解决方案。这些工具将被纳入未来安全性能更加强大稳固的控制系统中。这些系统架构，硬件和软件也都有可能被逐步商业化。

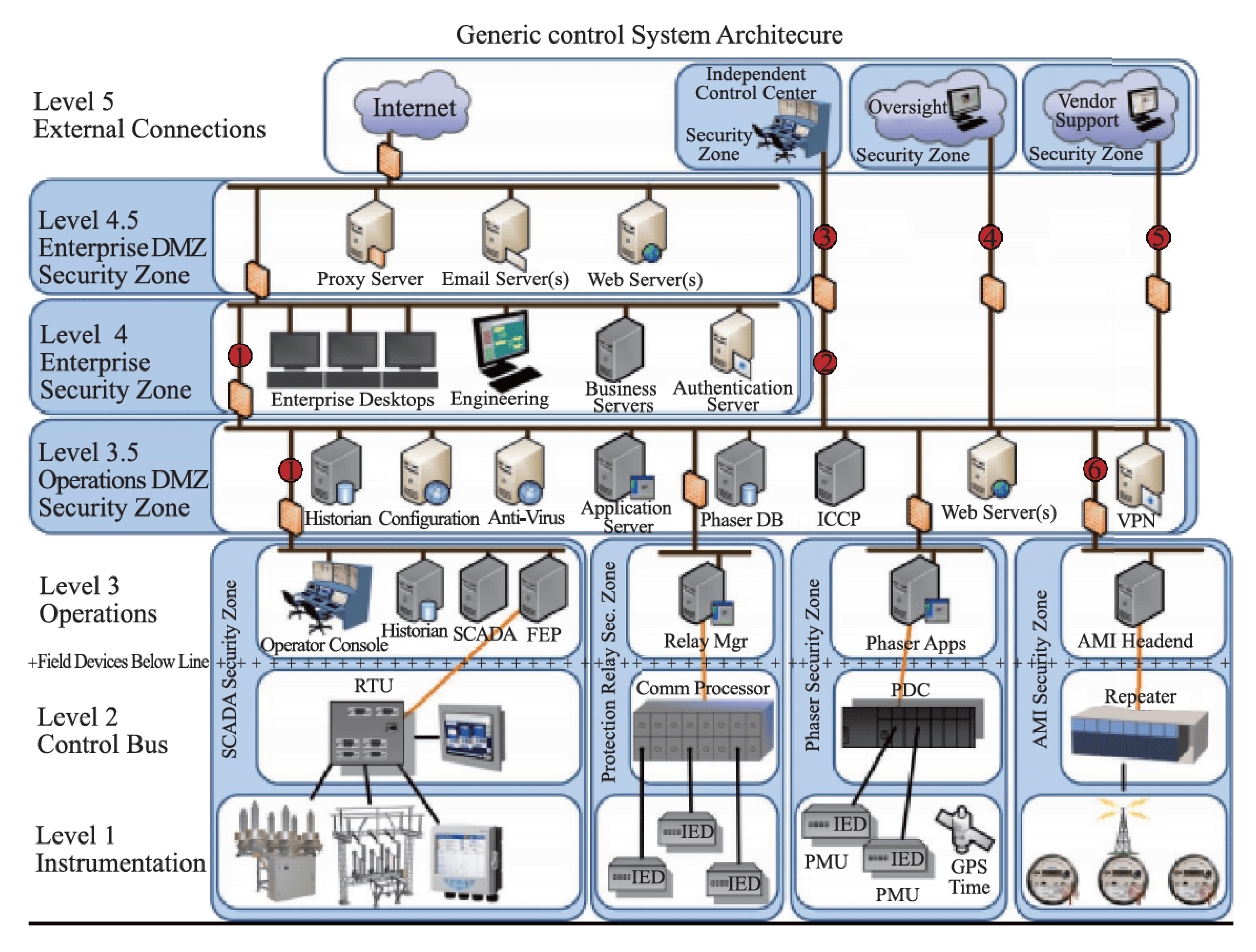


图 3-14　PNNL 提出的通用控制系统架构（来源：文献[10] Figure 2）

（3）PowerNET 测试床[11]

如图 3-15 所示的 PowerNET（Power Networking, Equipment, and Technology）测试床隶属于电网操作与规划技术集成能力套件（Grid Operation and Planning Technology Integrated Capabilities Suite，GridOPTICS）项目。GridOPTICS 项目是西北太平洋国家实验室下属的“未来电网倡议”项目（Future Power Grid

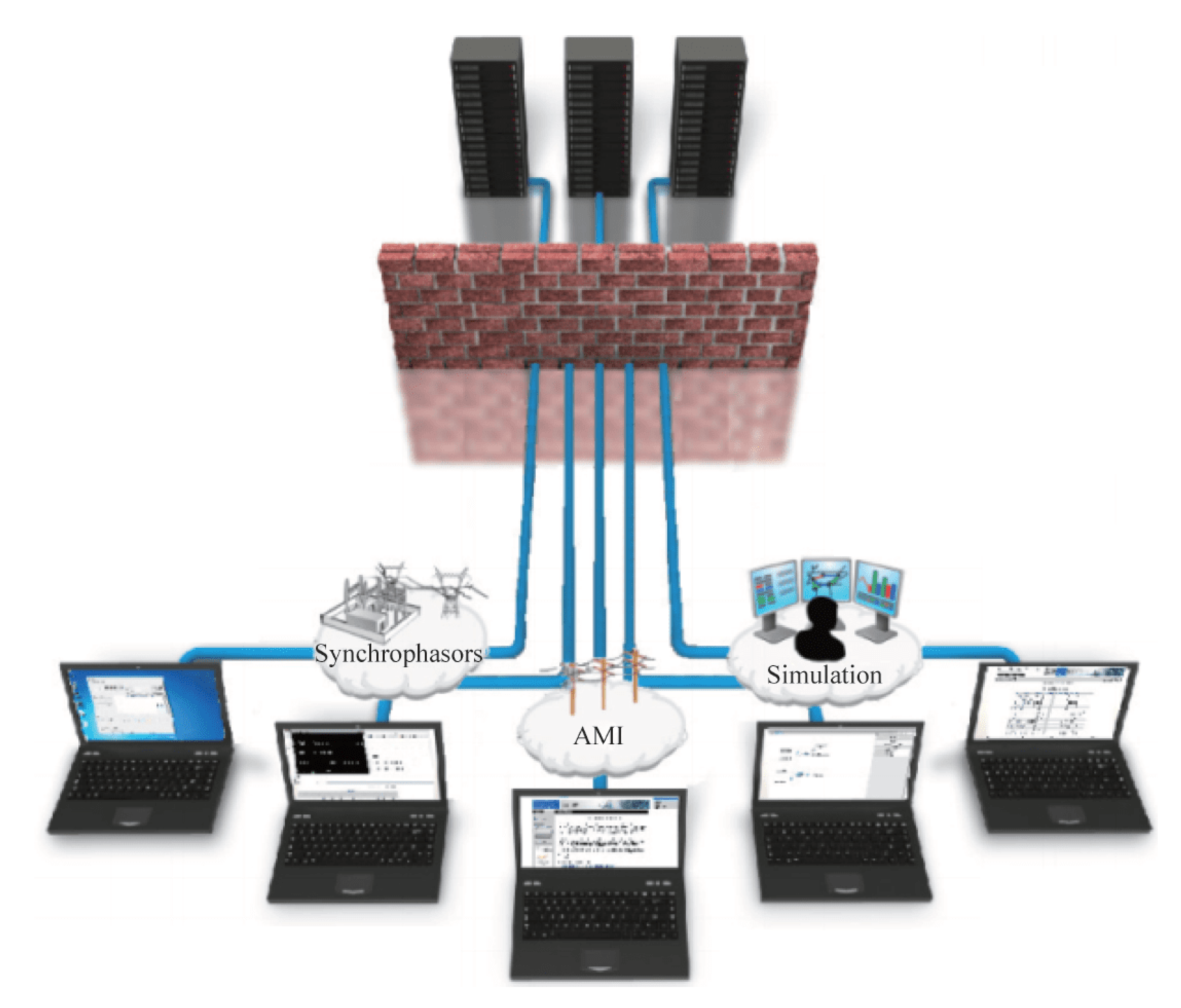


图 3-15 PNNL PowerNet 测试床(来源:文献[11])

Initiative,FPGI)的一部分。PowerNET 测试床为研究人员开发和测试新的想法提供了便利,并帮助厂商测试新设备和互操作性。该测试床还提供了一个电网共享资源,可降低非电力系统工程师与电力系统设备实验之间的技术壁垒。

具体地,PowerNET 测试床接入实时数据管理系统。该系统使用模型驱动类型的数据压缩、融合和复制算法来增强电网系统中信息网络的可靠性和可伸缩性。在 PowerNET 中,电网系统设备、仿真模块和虚拟仿真设备都集成到美国信息科学研究所研发的 DETER 软件中,以此来扩展 PowerNet 的仿真能力和范围。

3.3.3.4 橡树岭国家实验室

1. 实验室研究目标

在量子密钥分发方面,研究适用于能源行业系统的量子密钥分发机制,旨在

通过改进传统的量子密钥分发机制来进一步降低开销。研发一种新型量子密钥分发机制，允许多个客户端通过一个量子通信信道使用低成本的量子调节器来进行密钥分发。在下一代安全智能电网设计与实现方面，研究智能电网的可扩展通信网络技术，提高电网的可扩展性和自我配置能力，实现多用户多设备无缝连接。

2. 实验室研究内容

在量子密钥分发方面，由橡树岭国家实验室、通用电气全球研发中心和 ID Quantique 公司共同研究了量子密钥分发（Accessible QKD for Cost-Effective Secret Sharing，AQCESS）机制。橡树岭国家实验室主要负责研究可行的量子密钥分发协议，并负责系统集成工作。通用电气全球研发中心负责提供电力系统设备。ID Quantique 公司负责研发量子密钥系统和技术。本项目拟开发并展示一种新型的可提高量子密钥分发的通用性和可访问性的量子密钥技术，并将此项技术应用到商用的电网仪表中。在下一代安全智能电网方面，研究了如何在下一代电网的通信网络中应用扩频技术来建立一个较宽的通信带宽，提高网络的可扩展性能。

3. 主要成果

（1）验证了量子密钥分发信号调制解调操作和 AQCESS 通信节点；

（2）经调研后确定了通用设备的选型，选定了用通用电气公司的 JungleMUX 设备来开发原型系统；

（3）完成了原型系统的设计与开发；

（4）研究了电网底层安全通信机制，通过橡树岭实验室研发的混合扩频技术实现了电网物理层和 MAC 层安全通信；

（5）为智能电网应用程序，设计完成了混合扩频/CDMA 收发器，提高了电网网络的可扩展性。

3.3.3.5 阿贡国家实验室

1. 实验室研究目标

阿贡国家实验室（ANL）针对当前时代的可持续能源、健康环境和安全国家方面面临的重大挑战问题，研究 SCADA 系统安全，力争取得具有世界先进性的理论和工程成果。

2. 实验室研究内容

ANL 关于工业控制安全的研究主要集中在 SCADA 系统领域(主要是美国天然气管道运输的 SCADA 系统)。ANL 已经开展 SCADA 系统调查和评估研究,并开发出各种工具、技术和方法,用于评估和改进 SCADA 系统。ANL 还为天然气管道运输系统设计了 SCADA 远程设备控制方案。此外,实验室还通过 ISA 工作组来制定控制系统标准,包括 IEC 61850 标准等。

3.3.3.6 洛斯阿拉莫斯国家实验室

1. 实验室研究目标

通过卓越的科研成果来解决国家能源安全面临的挑战。实验室目前拥有的基础设施包括:1280 座建筑(包括 11 个核设施),道路总长 268 英里(已铺设 100 英里),电力线缆共计 34 英里,天然气管线共计 63 英里,此外还拥有一座电厂。

2. 实验室研究内容

实验室研究工作分两大类:①武器研究,包括开发满足目前军事需要的核弹头、设计试验先进技术方案;②非武器研究,包括核裂变、核聚变、中等物理加速、超导、生物医学、非核能及基础能源科学等。

在 NSTB 项目中,实验室主要负责在能源系统(如电网系统)中,研究如何利用量子密钥分发机制来进行密钥协商和交换,以此得到可用于传统加密认证算法中的密钥。

3.3.3.7 劳伦斯伯克利国家实验室

1. 实验室研究目标

实验室走在世界科学领域的最前沿,致力于研究先进科学技术,培养科研人才,推动美国和全世界的技术创新。

在 NSTB 中,实验室为设备之间发送和接收到的指令提供数据完整性保护机制,确保设备的网络安全和物理安全。利用传感器或执行器实现系统运行状态监测,并提供安全防御和保护机制。

2. 实验室研究内容

实验室的研究领域广泛,研究内容涉及生物医学、计算机科学、地球和环境科学、能源科学、能源技术、物理科学等领域。

在 NSTB 项目中，实验室主要负责根据基础设施系统中的设备运行过程中的物理资源限制条件及运行协议规范，研究系统和设备的运行状态监测机制。当存在来自系统外部或内部的安全威胁时，分析并识别有悖于既定协议规范的异常情况。

3.3.4　NSTB 承担项目

NSTB 包含多个项目，如表 3-2 所示，根据各个项目的目标，NSTB 项目可以分为三个方向：下一代控制系统、综合风险分析、系统脆弱性评估[6]。

表 3-2　NSTB 承担项目概况表

序号	项目名称	负责人	单位
一、下一代控制系统			
1	无线 Wireless	Jeff Dagle	PNNL 西北太平洋国家实验室
2	智能电网安全特征 Smart Grid Security Attributes	Jeff Dagle	PNNL 西北太平洋国家实验室
3	数据传输 Data Transfer Project	Jeff Dagle	PNNL 西北太平洋国家实验室
4	安全 SCADA 通信协议（SSCP）的协议分析仪 Protocol Analyzer for the SSCP	Mark Hadley	PNNL 西北太平洋国家实验室
5	密码的可信管理 Cryptographic Trust Management	Jeff Dagle	PNNL 西北太平洋国家实验室
6	现场设备的集中配置管理 Centralized Configuration Management for Field Devices	Jeff Dagle	PNNL 西北太平洋国家实验室
7	使用信任锚方式保护过程控制系统免受生命周期攻击 Protecting Process Control Systems Against Lifecycle Attacks Using Trust Anchors	Adrian Chavez	SNL 桑迪亚国家实验室
8	控制系统网络的异常检测和分布式主动响应 Anomaly Detection and Distributed Active Response for Control Systems Networks	Louris Wilder	ORNL 橡树岭国家实验室

续表

序号	项目名称	负责人	单位
一、下一代控制系统			
9	关键基础设施节点的可信任的无线传输 Trustworthy Wireless for Critical Infrastructure Sites	Wayne Manges	ORNL 橡树岭国家实验室
10	未来国家电网条件下的过程控制安全 Process Control Security under Future National Grid Conditions	Steve Fernandez	ORNL 橡树岭国家实验室
11	网络-物理攻击和网络-物理安全：第二道防线 Cyber-Physical Attacks and Cyber-Physical Security：The Second Line of Defense	James Nutaro	ORNL 橡树岭国家实验室
12	使用便携式验收测试仪和协议的SCADA系统网络安全测试 SCADA Systems Cyber Security Testing Through Portable Acceptance Test	Wayne Manges	ORNL 橡树岭国家实验室
13	网络安全审计和攻击检测工具包 Cyber Security Audit & Attack Detection Toolkit	Dale Peterson	Digital Bond，Inc
14	能源行业的威胁检测和分析 Detection and Analysis of Threats to the Energy Sector (DATES)	Alfonso Valdes	SRI International 斯坦福国际研究院
15	利姆诺斯可互操作的安全方案 Lemnos Interoperable Security Program	Vishant Shah	EnerNex Corp
16	保护智能分布式电网免受网络攻击 Protecting Intelligent Distributed Power Grids from Cyber Attack	Dr. Dong Wei	Siemens Corporate Research 西门子研究中心
17	标志项目 Hallmark Project	Rhett Smith	Schweitzer Engineering Laboratories，Inc 施瓦茨工程实验室

续表

序号	项目名称	负责人	单位
二、综合风险分析			
18	威胁特征分析 Threat Characterization	J. Michalski	SNL 桑迪亚国家实验室
19	实时安全状态可视化工具 Real Time Security State Visualization Tool	PNNL	PNNL 西北太平洋国家实验室
20	虚拟控制系统环境 Virtual Control System Environment (VCSE)	R. Halbgewachs	SNL 桑迪亚国家实验室
21	网络攻击对控制系统的影响分析 Impact Analysis of Cyber Attacks on Control Systems	J. Stamp & R. Laviolette	SNL 桑迪亚国家实验室
22	后果建模工具 Consequence Modeling Tool	B. Richardson Lozanne Chavez Lane Yarrington	SNL 桑迪亚国家实验室
三、系统脆弱性评估			
23	常见系统漏洞分析 Common Vulnerability Report	Chaffin	INL 爱达荷国家实验室

3.3.4.1　下一代控制系统

控制系统的网络攻击持续发展,能源部门必须有能力应对这些攻击。长期来看,能源控制系统安全建设需要下一代控制系统(next-generation control systems)安全技术的支撑。这些下一代安全技术包括:智能、内生安全及可靠控制系统体系结构、软件和硬件;高级的设备到设备的认证;准确高效的入侵检测和防御机制、事件关联和响应机制;在远端设备和监控中心之间、办公网络和控制网络之间的控制和系统通信安全协议。

1. 设计目标

下一代控制系统有两个研究目标:

(1) 研究远端设备和控制中心之间可扩展、高性价比的安全通信方法。开发保护边界数据安全传输的解决方案,并加速其推广和应用。

（2）设计对主机影响最小的可扩展、高性价比的新型安全架构和通信方式。加速技术成果转化，显著提高能源控制系统的网络安全等级。

2. 技术需求和挑战

在控制系统网络、远程设备和商用网络之间的通信连接网络十分重要，但以往的设计往往没有或很少考虑到这一点，其中存在着大量的网络安全漏洞。其次，每一个新的连接点都会增加基础设施的复杂度，并极易被攻击者利用而创建新的攻击向量。此外，能源部门大量地应用商业现货（COST）技术、标准化操作系统和在控制网络中依赖开放通信协议，这些也大大增加了工控网络的风险。然而，目前解决这些问题的安全技术在安全事件期间会大大降低系统性能和减缓系统的响应，这也违背了安全设计者的初衷。

针对这些问题和挑战，工业控制系统中的安全需求主要有以下几点：

（1）不影响现有系统的、性价比和鲁棒性高的 SCADA 加密设备。

（2）安全的即插即用控制系统组件。

（3）集成防火墙、入侵检测和防病毒功能为一身，且对主机影响最小的高性价比网关安全技术。

（4）具有自动报告功能的入侵检测和防御技术。

（5）安全的事件管理和取证工具。

（6）自动化的安全状态监测和响应系统。

（7）改善系统通信性能，启用对系统影响最小的安全解决方案。

3. 项目里程碑

根据项目目标，下一代控制系统实施过程中具有 6 个标志性的事件，如图 3-16 所示。对于第一个设计目标，计划分四个步骤实现，对应于图中的事件 1 到事件 4；

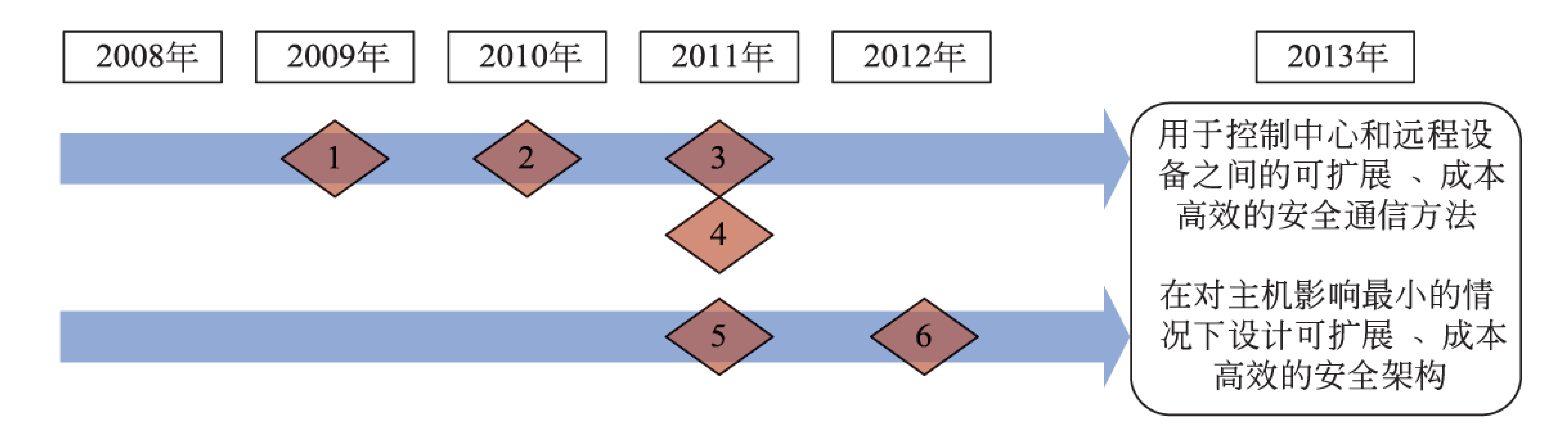


图 3-16 下一代控制系统里程碑和性能目标

对于第二个设计目标，计划分两个步骤实现，对应于图中的事件5和事件6。这6个事件的描述如下：

(1) 和工业产品供应商一起现场测试串行协议认证技术。

(2) 将串行协议认证技术转让给商业供应商。

(3) 和工业合作伙伴一起现场测试可互操作的控制系统安全体系架构。

(4) 将可互操作的控制系统安全体系框架转让给商业供应商。

(5) 演示为控制系统应用设计的集成的入侵检测、防御和事件关联能力。

(6) 将集成的入侵检测、防御和事件关联技术转让给商业供应商。

4. 主要项目介绍

(1) 现场设备的集中配置管理(Centralized Configuration Management for Field Devices)[5]

① 项目目标

项目的主要目的是开发一个独立于供应商的应用软件，能够使用户可以在监控中心实现对所有现场设备的管理和配置。

② 技术方法

本项目将使用安全SCADA传输协议(SSCP)作为传输配置变更信息的传输机制。SSCP库包含加密和授权功能。SSCP还被设计为能够利用专有的加密密钥对来实现加密并且其加密过的数据可以在现有传输媒介上进行传输。安全SCADA的数据保护方式是由信息的类型决定的，例如，工程访问数据可以使用加密和授权保护；SCADA数据只需使用加密操作。这提供了非常好的安全性和灵活性。本项目也使用西北太平洋实验室的电力基础设施运营中心的平台和多个厂商的设备作为研究和开发环境。

(2) 关键基础设施节点的可信任的无线传输(Trustworthy Wireless for Critical Infrastructure Sites)[5]

① 项目目标

研发网络级、主机级和设备级的入侵检测系统，建立安全事件关联模型，搭建一个全行业的、分布式的并具有隐私保护功能的安全事件数据共享平台。

② 技术路线

第一步，重点关注电力行业，支持ISA100标准(无线工业自动化)无线可信技术标准制定工作。每年工作组至少每两个月进行一次电话会议和面对面的会议。

第二步，探讨在关键基础设施制定的节点中部署无线技术中企业政策、法规等内容。撰写一份描述关键基础设施无线系统高安全性、高可靠性的文档，文档中需要通过吞吐量、范围、延迟和安全等指标来量化无线通信可靠性。

第三步，促使 ISA100 可信赖无线工作组（Trustworthy Wireless Working Group，TWWG）制定"无线工业自动化可靠性"草案。在 SCADA 原型系统环境下利用无线笔记本进行漏洞测试，并出具一份详细测试报告。

(3) 能源行业的威胁检测和分析（Detection and Analysis of Threats to the Energy Sector，DATES）[12]

① 项目目标

研发网络级、主机级和设备级的入侵检测系统，建立安全事件关联模型，搭建一个分布式的具有隐私保护的安全事件数据共享平台。

② 技术路线

第一阶段：研究控制系统存在的安全脆弱性，决定如何最优化地部署和设计入侵检测传感器。综合利用入侵检测组件和企业安全管理工具来建设全面的安全事件管理能力。为入侵检测系统研发安全事件关联模型。通过建立一个安全的、匿名的信息共享传输通道来增强网络威胁分析能力，并建立维护一个全球性的安全事件信息共享平台。

第二阶段：选择适当的入侵检测组件，并创建安全事件关联规则集合。建立攻击场景来验证安全事件关联系统的有效性，并验证系统的安全态势感知能力。

第三阶段：分析并完成系统配置，以此来最大化系统检测安全攻击的能力。组织建立攻击团队来对系统进行攻击实验，验证系统的入侵检测能力。

③ DATES 测试床介绍

DATES 测试床由英维斯（Invensys）的 DCS 和桑迪亚国家实验室的 VCSE 两部分组成。Invensys DCS 测试床主要是由 Invensys DCS 以及上位机 IA 系统组成。Invensys DCS 系统对 Modbus 协议进行了测试。VCSE 测试床对办公网和隔离区进行了仿真。

DATES 测试床主要用于分析网络信息系统及其威胁的相关性。系统主要是用虚拟机技术实现真实的系统组件，能够在一台主机上运行一个小型的 SCADA 网络。两个实验室之间采用安全隧道进行数据传输。DATES 测试床的结构图如图 3-17 所示。

Invensys DCS 测试床与 VCSE 测试床之间的配置及数据传输关系如图 3-18 所示。图 3-19 给出了在控制系统和商业数据库上进行威胁检测的 IDS 部署位置。

图 3-17　DATES 测试床结构图(来源：文献[12] Figure 17)

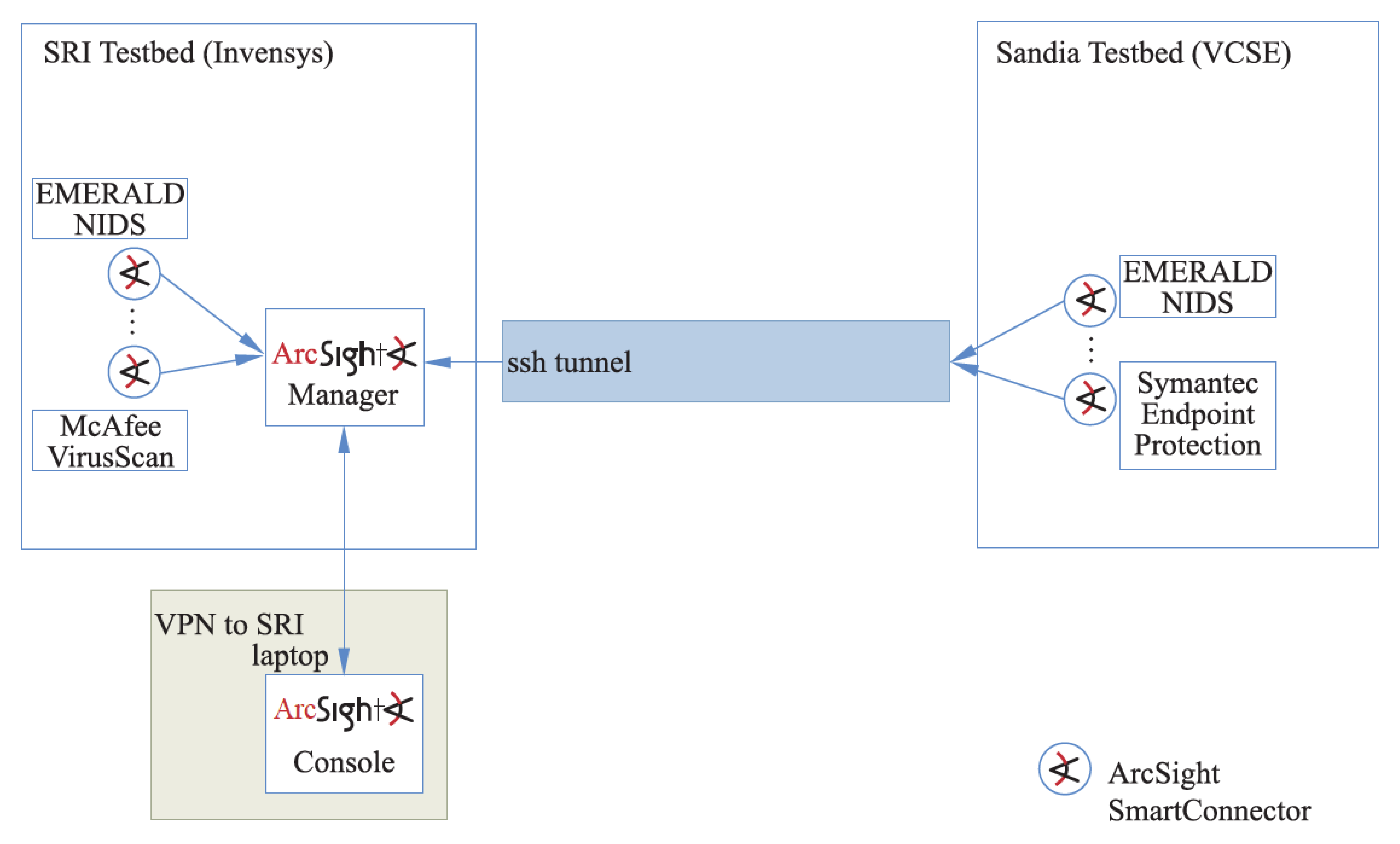


图 3-18　Invensys DCS 与 VCSE 之间的配置及数据传输关系图(来源：文献[12] Figure 18)

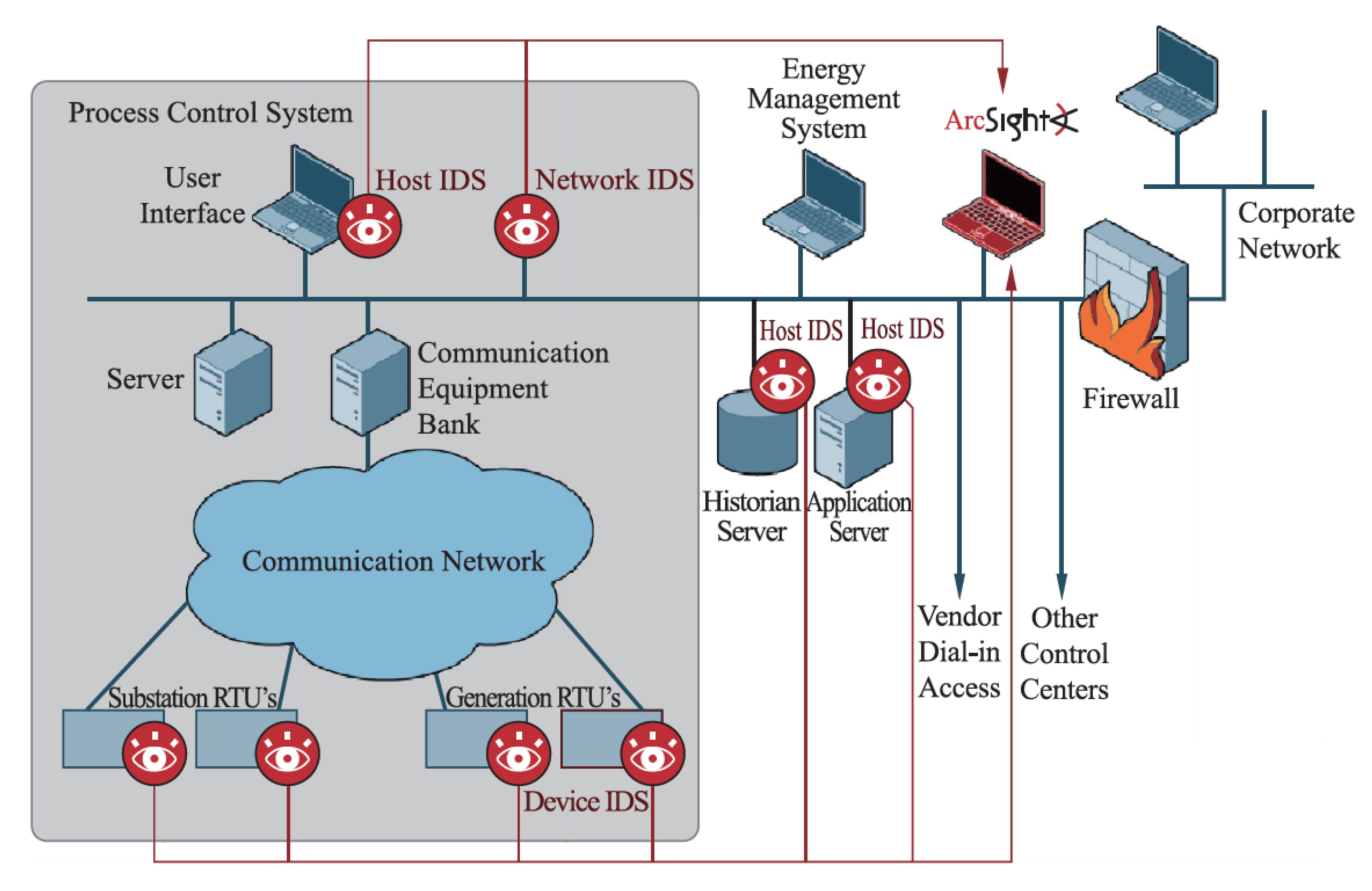


图 3-19 DATES 测试床 IDS 部署位置示意图(来源：文献[12] Figure 1)

DDoS 攻击的可视化分析结果如图 3-20 所示。红色正方形代表 DDoS 的源 IP 地址，紫色正方形表示该 IP 地址可能受到的 DDoS 攻击。每个源地址和目的地址之间的箭头都表示一类事件。浅蓝色的圆圈表示事件数量的多少。

(4) 保护智能分布式电网免受网络攻击(Protecting Intelligent Distributed Power Grids against Cyber Attack)[13]

① 项目目标

本项目主要是针对智能电网开发一个分层的网络安全系统，开发电网物理硬件的自动化风险评估功能，使用高级仿真、机器学习和动态进化技术，基于模拟演习和历史攻击数据来识别网络安全威胁。该分层的网络安全系统主要由现场设备或者控制器的安全代理、自动控制层的安全路由器和电网层的安全管理系统三部分。安全代理主要是用来进行简单日志记录、报告和检测；安全路由器主要是管理数据流量、使用既定的网络规则来检测入侵行为；安全管理系统主要是在基于仿真和历史信息的基础上更新改进现有安全策略或是制定新的安全策略。管理系统将会连接交换机和代理服务器，作为一个认证、授权和计费(Authentication, Authorization and Accounting, AAA)的服务器运行，当系统获得新的安全补丁时，AAA 服务器会将它们分发到控制系统组件中。

② 技术路线

这种智能分布式的分层方法能够为先进的电网提供一个完整的安全解决方

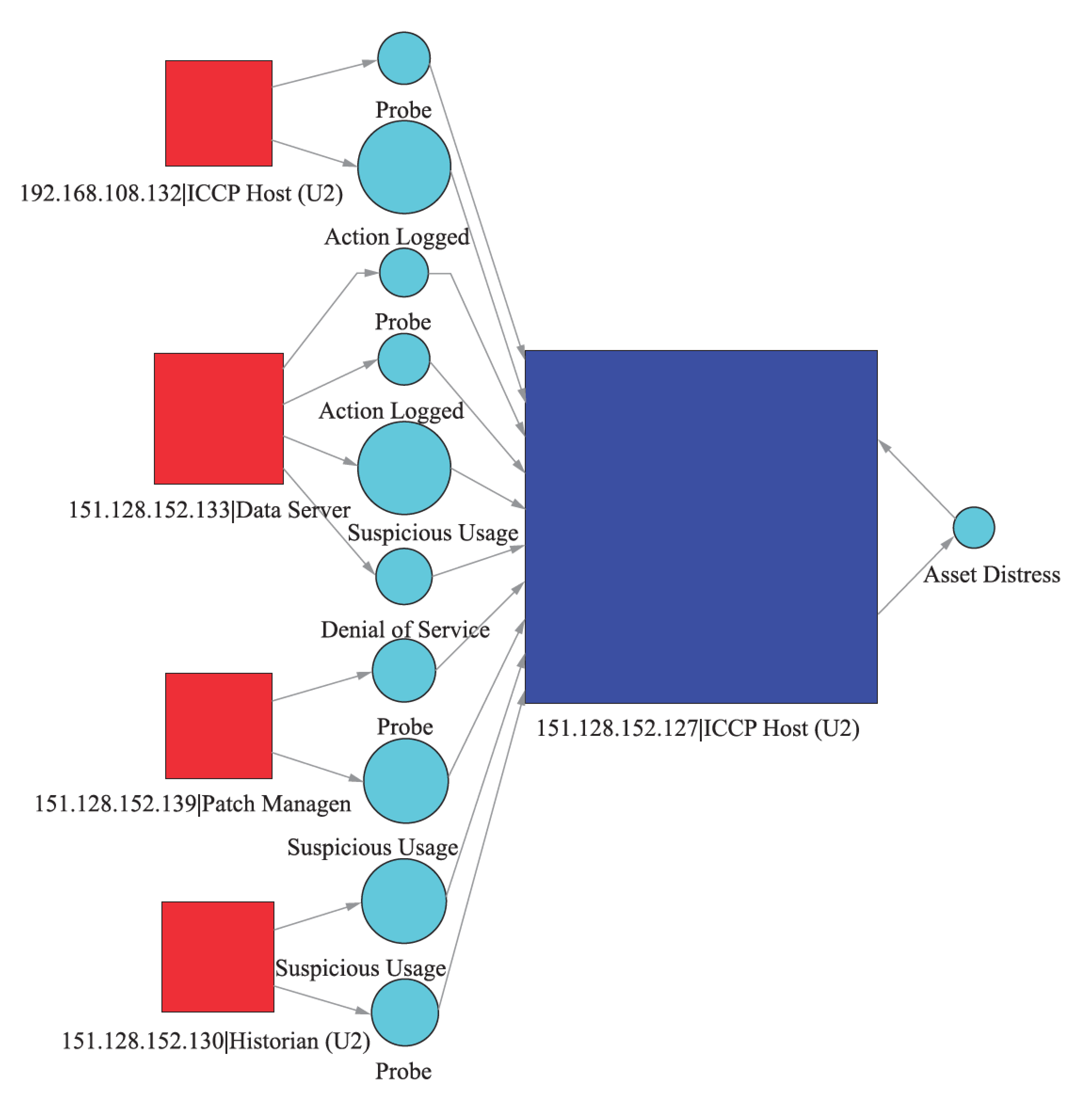


图 3-20　DDoS 攻击结果图(来源：文献[12] Figure 21)

案。本项目主要包含两个阶段。

第一阶段(设计和开发)：分析电力控制网络的网络攻击的影响，研究发展基于风险的关键资产识别模型和算法，并最终完成关键资产识别系统的搭建。

第二阶段(测试和验证)：在爱达荷实验室，对此系统的安全代理、安全路由器、安全管理和安全集成配置软件进行两轮测试。

电网安全建议的 3 层框架结构如图 3-21 所示。包括电网层、自动控制层和安全层。电网层由各类电力现场设备组成，自动化控制层负责监视和控制电网层，安全层提供明确的责任划分和安全功能，这些功能在设计上相互独立。

图 3-22 显示了 4 种安全代理的位置。第一种代理是独立的设备，其具有两个网络接口，其中内部端口连接到远程终端单元(remote terminal unit，RTU)

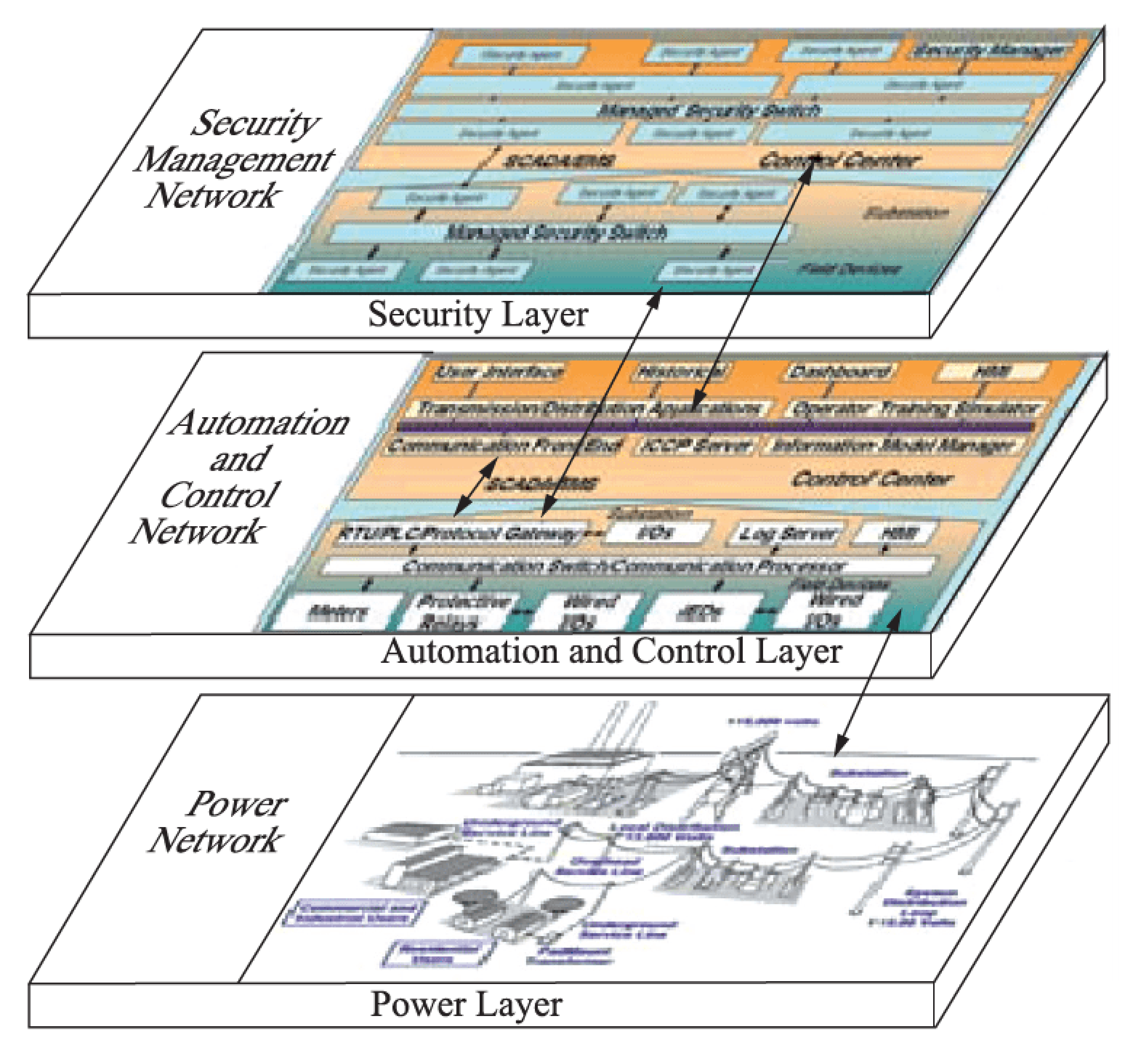


图 3-21　电网 3 层架构图(来源：文献[13] Figure 3)

EMS
Security Agent
Control Center
Public Network
RTU/PLC
Security Agent
Log Server Security Agent
1
3
4
Security Switch
Security Agent
Security Agent
Security Agent
Security Agent
2
IEDs
Protective Relays
Meter
Meter
……
Meter
I/O
I/O
I/O
PTs
CTs
PTs
CTs
PTs
CTs
Substation

图 3-22　4 种安全代理位置示意图(来源：文献[13] Figure 6)

或 HMI 等需要保护的设备，外部端口连接到交换机或路由器等网络设备上。第二种代理也是独立的设备，同样具有两个网络接口，其中内部端口连接到一组电气设备上（如测量仪表或者受保护的继电器），外部端口连接到网络设备上（如交换机、路由器）。第三种代理集成在一个管理型的交换机上，在内部端口上运行虚拟的安全代理。第四种代理架设在新加的设备上（如日志服务器、PLC、RTU），这些新加入的设备独立运行。

3.3.4.2　综合风险分析

根据 NSTB 项目的定义，综合风险分析（integrated risk analysis）是指通过收集能源控制系统的网络安全威胁、脆弱性和安全后果等方面信息，来分析能源行业网络安全态势。对能源控制系统进行综合风险分析需要一整套安全建模和分析工具。准确的风险评估能使能源行业利益相关者优先考虑关键网络资产的安全需求，并将有限的资源集中用于解决最紧迫的安全问题。

1. 设计目标

NSTB 设定了以下两个方面设计目标：

第一，建立能源行业系统的网络安全威胁、脆弱性和安全后果分析能力。研究侧重于分别对小、中、大规模集成网络系统的威胁场景进行模拟、识别与展示。在这些场景中，综合风险分析需要系统的端到端的方式来判断风险特征，并以此确定最佳安全行动时机和方案。

第二，研发用于控制系统仿真和评估安全威胁减缓措施的可扩展虚拟控制系统模拟工具。研究工作包括开发一个经济实用的控制系统模拟工具，分析系统安全态势感知模型的鲁棒性，评估系统采用安全防护措施后对系统正常运转所带来的影响。

2. 技术需求和挑战

安全风险仿真和建模工具可以用来模拟现实世界能源行业网络安全攻击场景，以此来预测安全攻击后果和不同行业之间的级联故障影响效果。此外，这些工具还可以用来测试、评判新安全技术的有效性。由于缺乏此类工具，人们目前无法实现对能源行业系统网络风险的量化分析和理解。因此，综合风险分析项目需要研发网络攻击和应急响应仿真工具，建立一种能源控制系统安全态势基准，开发具有内置测试框架和指南的安全测试工具。但是，在具体的研发工作中存在以下技术挑战：

(1) 创建一个安全风险矩阵。该矩阵折中综合量化现实网络攻击场景中的网络安全威胁、脆弱性和安全后果因素。网络安全威胁、脆弱性和安全后果每个方面的精确量化就不易实现，所以综合这三方面因素的量化工作会更加困难。

(2) 研发控制系统网络安全风险评估工具。该工具包括工控系统功能优先级排序和安全成本核算功能。能源控制系统复杂，功能繁多，实现优先级排序需要对能源系统进行深入的系统分析和功能分解，实现安全成本核算则需要对系统安全防护措施及其安全效果有一个清晰准确的理解。这些工作在技术层面都存在一定的难度。

3. 项目里程碑

图 3-23 中的 7 个事件的含义分别为：

(1) 为能源行业识别出可能的控制系统网络威胁场景。

(2) 验证适用于小规模网络场景下的端到端安全威胁分析能力。

(3) 验证适用于中等规模网络环境下的端到端安全威胁分析能力。

(4) 验证安全评估工具(虚拟控制系统环境)的初始运行能力。

(5) 验证适用于大规模网络场景下的端到端安全威胁分析能力。

(6) 提供一种适用于能源系统或设备拥有者的端到端安全威胁分析能力。

(7) 提供一种能够用来为能源行业系统或设备拥有者的全功能虚拟控制系统环境工具。

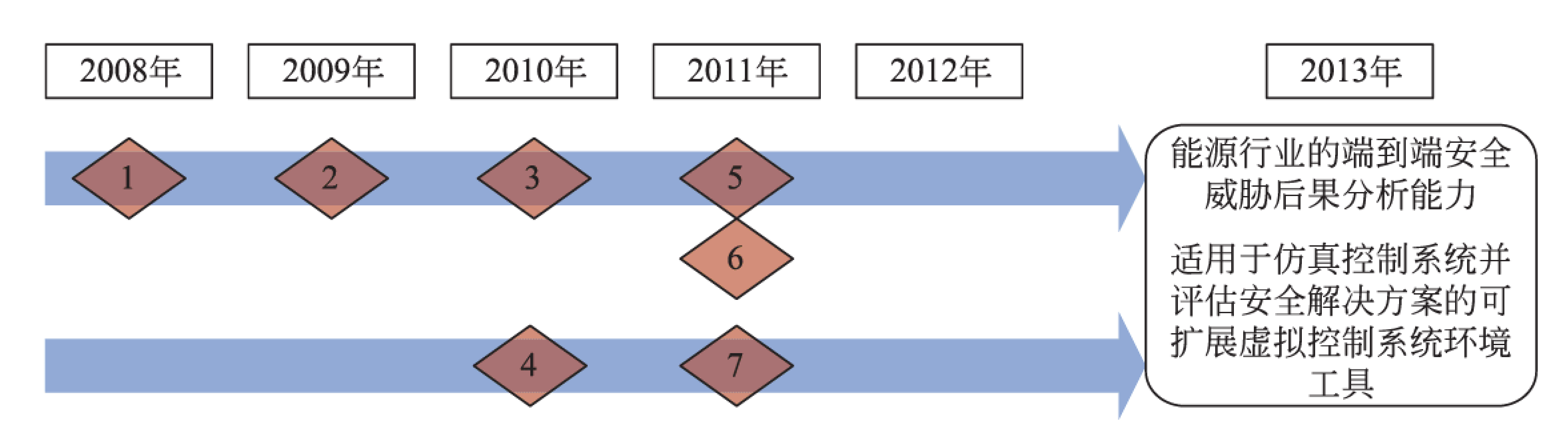


图 3-23 综合风险分析里程碑和性能目标

根据综合风险分析项目目标，本项目实施过程中在各财年设立了如下里程碑目标：

(1) 2008 财年：为能源部门确定合理的控制系统的网络威胁场景。

(2) 2009 财年：在小规模情况下，展示端到端的风险分析能力。

(3) 2010 财年：在中等规模情况下，展示端到端的风险分析能力。验证安全评估工具的初始运行能力——虚拟控制系统环境(VCSE)。

(4) 2011 财年：在大规模场景中，演示端到端的风险分析能力。为能源部门利益相关者提供一个完全集成的端到端安全威胁分析能力。对能源部门的利益相关者提供全功能 VCSE 工具。

4. 主要项目

(1) 虚拟控制系统环境(Virtual Control System Environment, VCSE)[14]

① VSCE 目标

VCSE 模型能够模拟控制系统的网络或物理系统及其所面临的安全威胁。这种模拟便于对控制系统可能遭受的威胁及其后果进行分析研究。VCSE 模型中的设备包括真实、半实物模拟和仿真三种类型(见图 3-24)。VCSE 中的安全威胁也包括真实和模拟两种形态的恶意软件。

② VCSE 工具箱

图 3-25 描述了 VCSE 建模者在一个典型网络物理系统中所关心的所有元素。VCSE 建模者可以设置该图中所示的每个元素，综合风险分析师则可以有选择性地重点关注那些与安全风险相关的元素。VCSE 工具箱主要包括人员、物理、模拟和仿真四类元素。其中，人员元素既可以表示真正的运营商、综合风险分析师和工程师，也可以表示恶意的攻击者。物理套件可以代表系统中各种设备、软件，以及模拟攻击的恶意软件，这些恶意软件已经成功集成到 VCSE 模型当中。半实物模拟套件拥有模拟控制器和接入仿真软件的接口，能够模拟混合异构网络。仿真套件内嵌了桑迪亚国家实验室研发的 Umbra 仿真软件的所有模型，并支持将这些模型集成到 VCSE 工具中。

在实际应用中，VCSE 已成为分析控制系统复杂威胁问题和物理信息系统安全设计的首选工具，该工具具有如下几类功能：

- 系统完整性验证。由于系统中的一些细节可能会对整个系统产生较大影响，开发系统完整性模型需要非常深入、全面的研究。VCSE 促进了这一过程，提供了一个容易理解的“完整性验证”系统模型，在模型开发过程中发挥着重要作用。
- 概念探索和验证。VCSE 模型作为真实系统的模拟，综合风险分析师可以安全地模拟执行攻击者可能对真实系统发起的任何攻击，并进行分析和理解。此外，综合风险分析师可以对尚未发现，但理论上可能存在的缺陷和漏洞进行建模与测试。
- 设计和测试。VCSE 模型提供了一个理想的环境，分析师可以使用真正的恶意软件对系统进行攻击，反复进行“设计—实施—测试”过程，以此分析确定系统漏洞的安全缓解技术。

图 3-24 信息物理系统典型系统图(来源：文献[14] Figure 1)

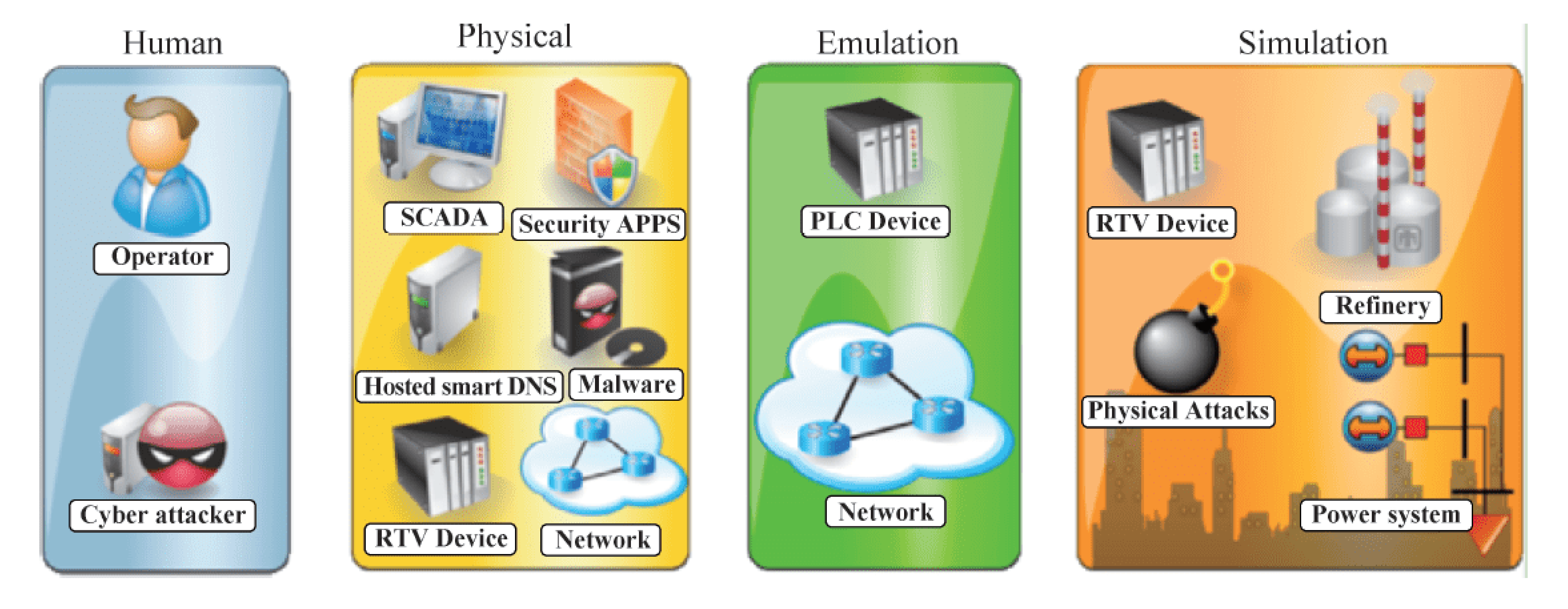


图 3-25 VCSE 工具箱(来源：文献[14] Figure 2)

③ VCSE 模型应用

根据 VCSE 模型，开发团队对一系列控制系统进行了模拟建模，并对其可能遭受的攻击及其后果进行模拟，具体模拟对象包括炼油厂 RTU、配电网络、燃烧炉系统 PLC 等设备、系统和网络。此外，在训练模式下，开发人员使用图形化敌手建模工具(Graphical Adversary Modeling Environment，GAME)的一个扩展版本驱动 Metasploit 工具，来逆向推出恶意软件代码。

图 3-26、图 3-27 和图 3-28 分别表示了小型炼油厂、电力配电系统和燃烧炉系统在遭受攻击前和攻击后的 VCSE 模型图。此外，VCSE 还模拟了如图 3-29 所示的 DNS 攻击对控制系统的影响。攻击者试图发布控制系统中 RTU 的虚假 IP 地址。一旦成功，SCADA 系统将终止对真实系统的连接，并连接到攻击者已经建立好的虚假控制系统。一旦上述转移创建成功，攻击者就能接管真实 SCADA 系统，并进一步实施控制。实际研究表明，VCSE 能通过对实际系统的模拟，从较小的方面进行较为全面的分析。分析师可以使用模型来确定攻击的影响程度，这一方式可以有效降低攻击的成本与风险。

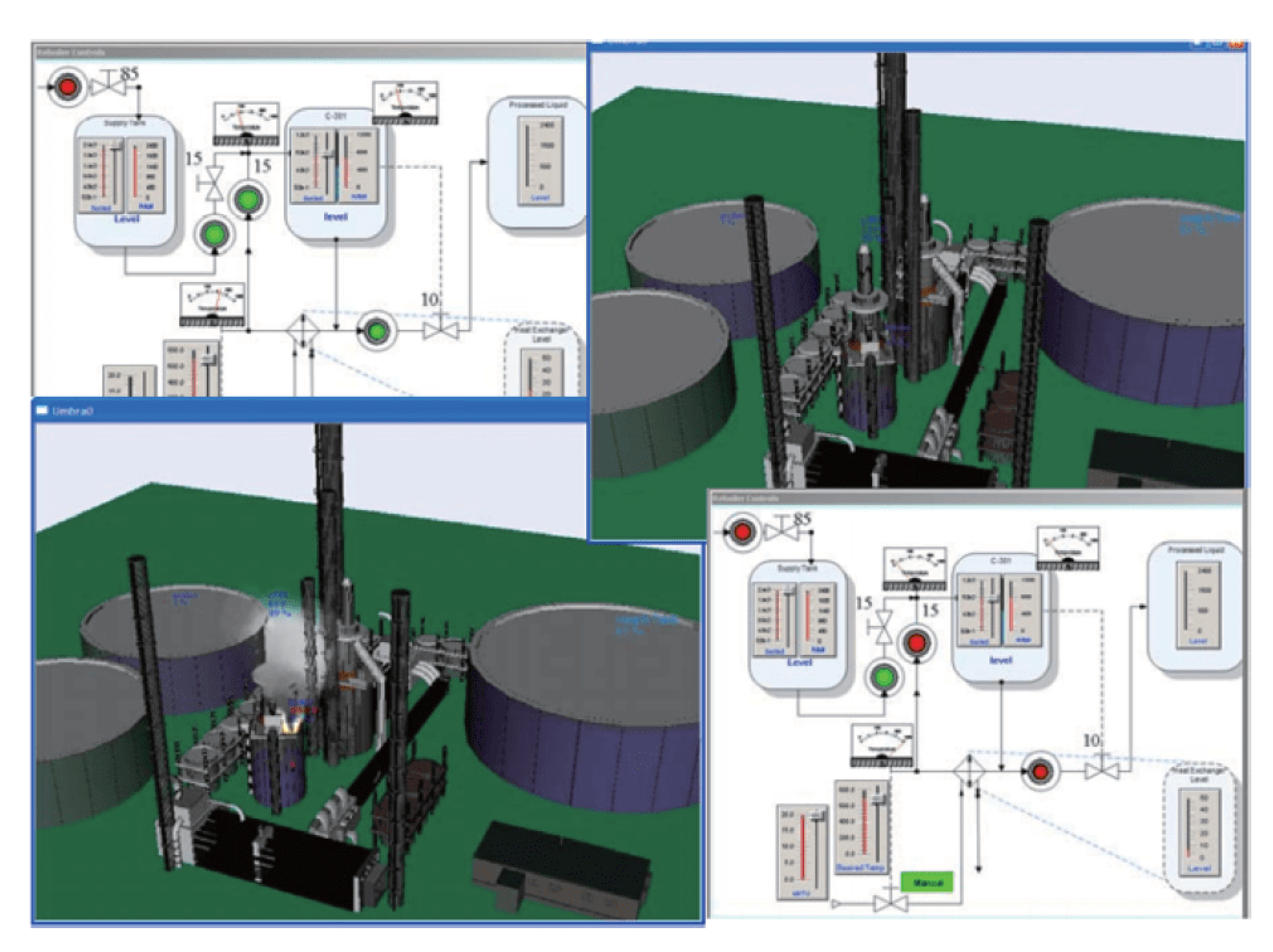


图 3-26　小型炼油厂在遭受网络攻击前和攻击后的 VCSE 模型图(来源：文献[14] Figure 3)

(2) 结果建模工具(Consequence Modeling Tool，CMT)[15]

① CMT 简介

由桑迪亚国家实验室与麻省理工学院共同建立的后果分析方法和框架为

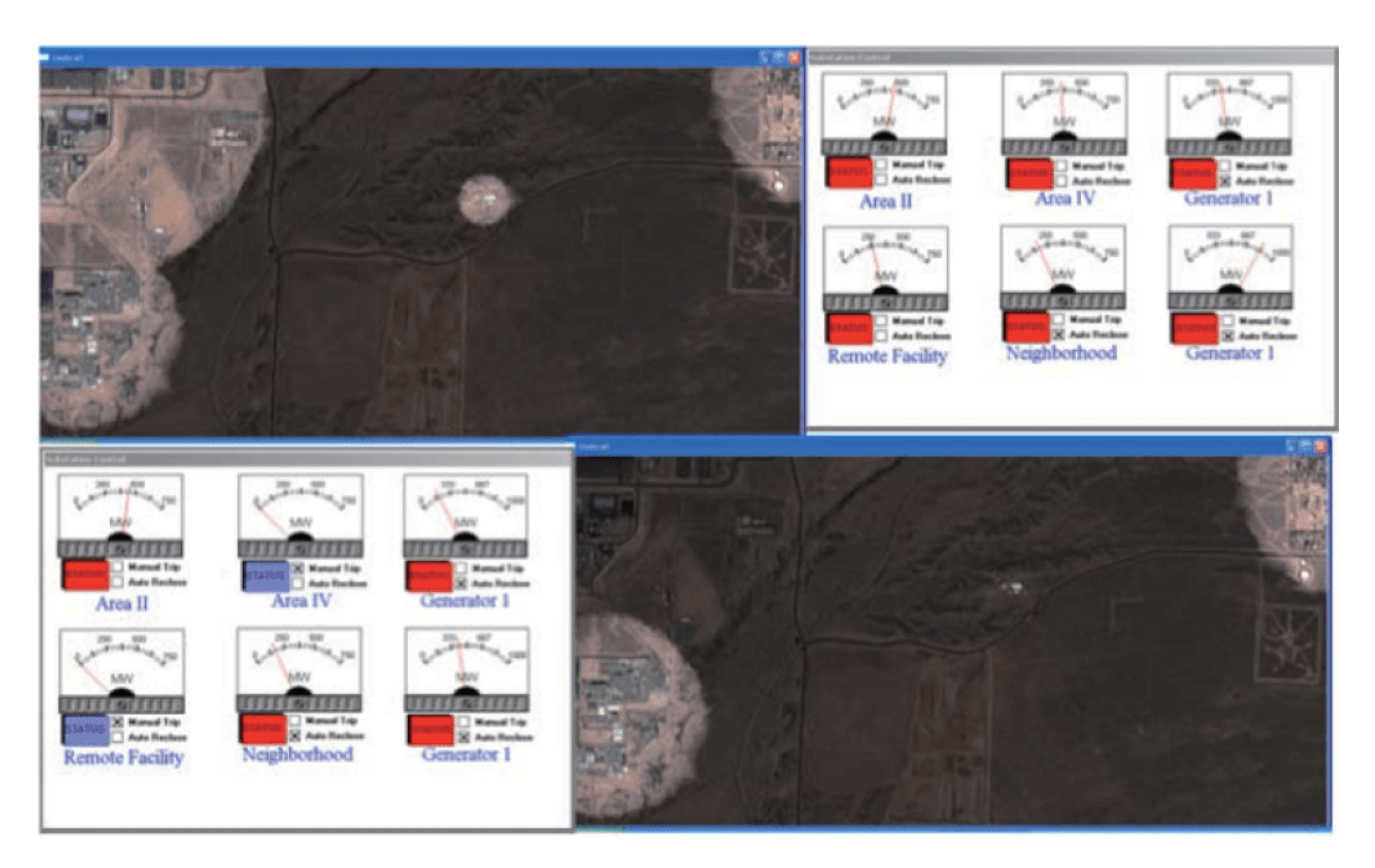


图 3-27 电力配电系统在遭受网络攻击前和攻击后的 VCSE 模型图(来源：文献[14] Figure 4)

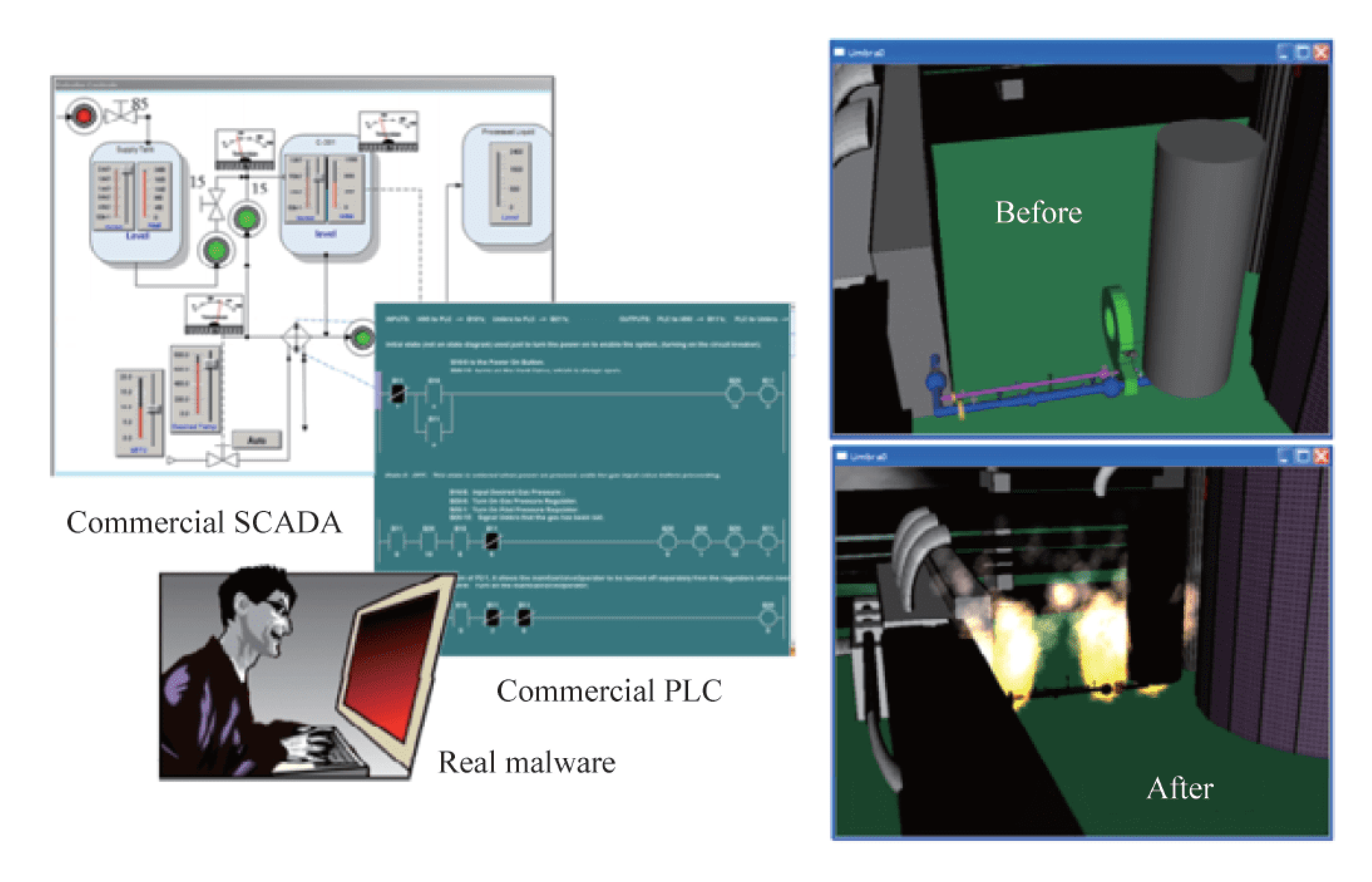


图 3-28 PLC 控制下的燃烧炉在遭受网络攻击前和攻击后的 VCSE 模型图
(来源：文献[14] Figure 5)

NSTB 的结果建模工具(CMT)项目提供了研究基础。该工具主要用于当地区域内电网建模。CMT 基于一个对环境、安全、经济等后果进行分类的实用性排名列表，并通过对系统内各个物理元素在遭受攻击时对系统产生的各类后果进

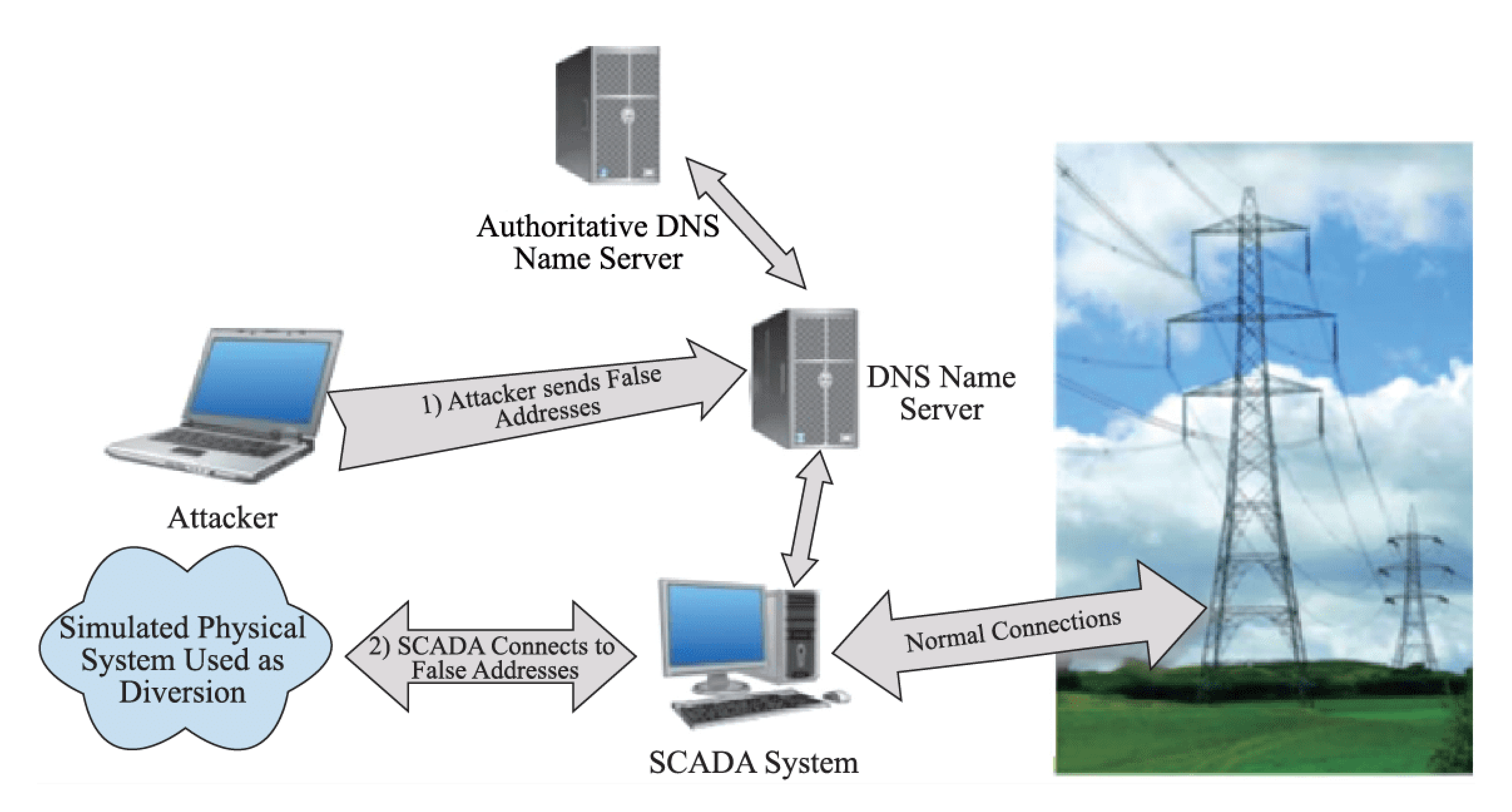


图 3-29　通过虚假 IP 地址发起的网络攻击（来源：文献[14] Figure 6）

行分析，生成一个价值树模型。同时，该工具还为处于威胁场景中的工控系统的总体安全后果提供了各类性能指标。通过这些信息，可以对出现在工控系统中的各类安全威胁的危害程度进行分析和排名。

在关键基础设施保护的领域，可以从本地、地区和国家层面进行后果分析，每个层面都可以考虑安全威胁对其他关键基础设施的级联影响及后果。为了识别工控系统可能遇到的威胁和攻击向量，CMT 可以在其遭受网络攻击时，对物理影响后果进行建模分析。

② 技术路线

首先，CMT 为基础设施利益相关者提供服务，帮助其对工控系统遭受网络攻击后果进行分析，主要分析基础设施停机所导致的资本支出、收入损失、民众的生活状态及情绪波动等几个维度的后果。

其次，定义或实现以下内容。即定义影响的类别；在各个类别，声明该影响对其他部门的重要性，定义该影响的安全对策；定义该影响与物理效应的关系；定义电力系统及其用户关系；定义在电力系统中产生的后果影响；创建价值树。

最后，通过结果分析引擎，分析系统中的任意功能，量化评估遭受网络攻击的后果。项目组利用结果排名架构进行软件开发，对分析引擎生成的报告进行评估，并以此建立价值树模型。这一工具能够对每一个威胁向量进行分析，并将其对系统各功能产生的影响进行评估。

③ 影响分类

为了构建价值树模型，首先需要对事件的影响类别进行定义。在图 3-30 所

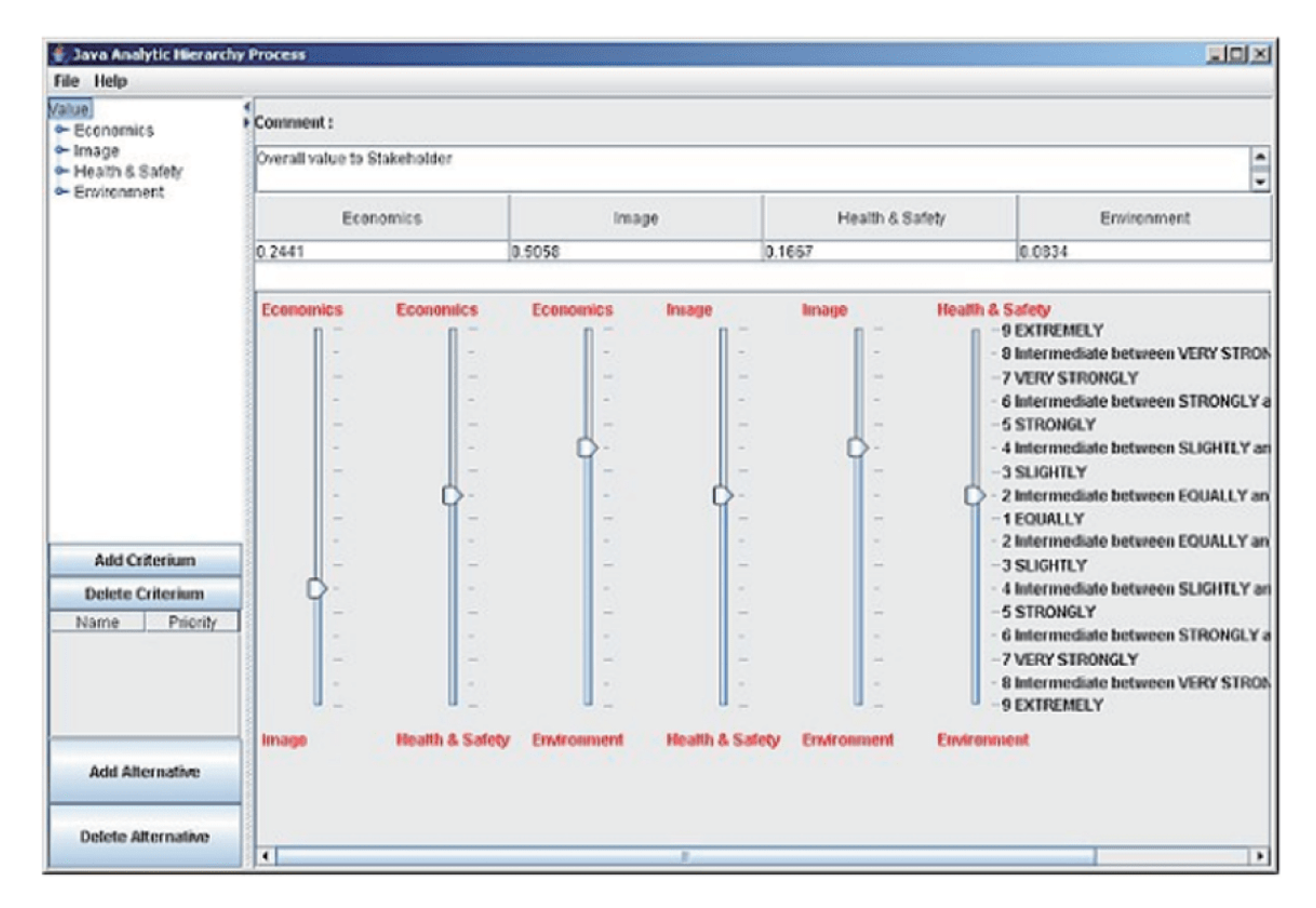


图 3-30 定义在 CMT 用户接口中，用于构建属性树的影响分类图（来源：文献[15] Figure 1）

示的例子中，影响类别被分为经济、形象、健康安全、环境这四个方面。对各个影响类别进行两两比较，将选定的两个目标的相对重要程度用 0～9 表示（0 代表重要性完全相同，数值越高，代表两者重要性差距越大）。通过这项评估可以分析出各个类别的相对重要性。

④ 表现评估

在对各种事件影响进行分类后，需要对每一类事件影响进行多方面的表现（或反馈）评估。图 3-31 的例子中，将事件影响从公众、客户、政治三方面进行评估。可以看出这一例事件的政治影响相对处于主要位置，对客户影响次之，对公众的影响相对较小。

⑤ 等级评定

在对事件影响的各项表现进行评估后，需要在各方面表现中进行事件等级的评定，以此来确定事件造成后果的严重程度及需要采取的后续措施。如图 3-32 所示，等级 0 代表事件几乎不会造成影响；等级 1 代表需要对工业规范进行小程度的政治干预；等级 2 代表需要一些政策推动，对工业标准及规范进行增补或修订；而等级 3 代表事件影响严重，亟须出台相关政策，对现有工业规范进行较大规模的改革。

图 3-31　定义在 CMT 用户接口中，用于构建属性树的性能测试图（来源：文献[15] Figure 2）

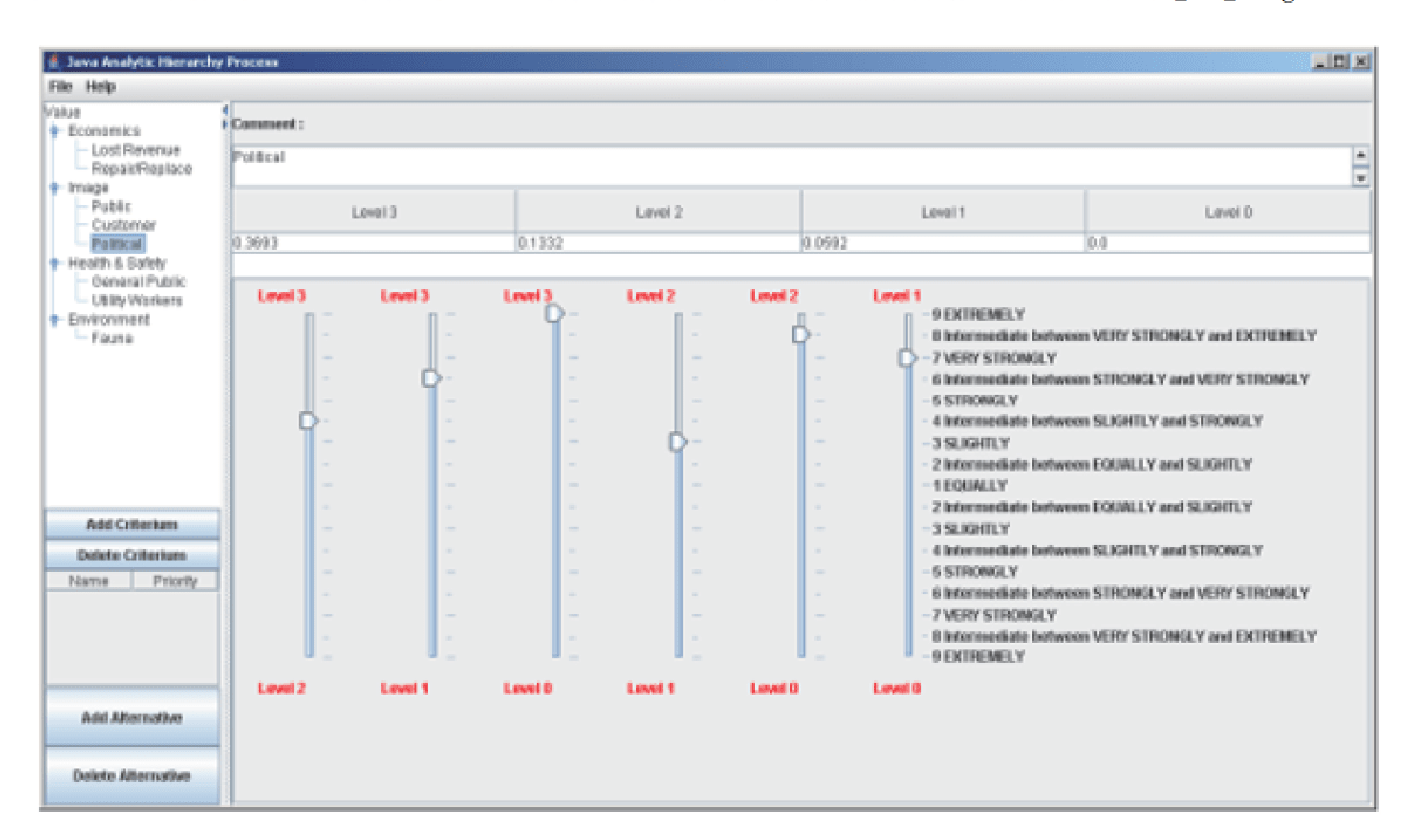


图 3-32　定义在 CMT 用户接口中，用于构建属性树的构建尺度图（来源：文献[15] Figure 3）

通过以上三方面的分析，可以构建价值树模型，以此对威胁向量可能造成的后果及影响进行全面的测量评估，以此对攻击事件进行全面评价，并制定应急措施。

⑥ CMT 用户界面

CMT 提供了如图 3-33 所示的用户界面，在结果建模框架下，为用户提供价值树模型、性能指标、后果分析等信息。

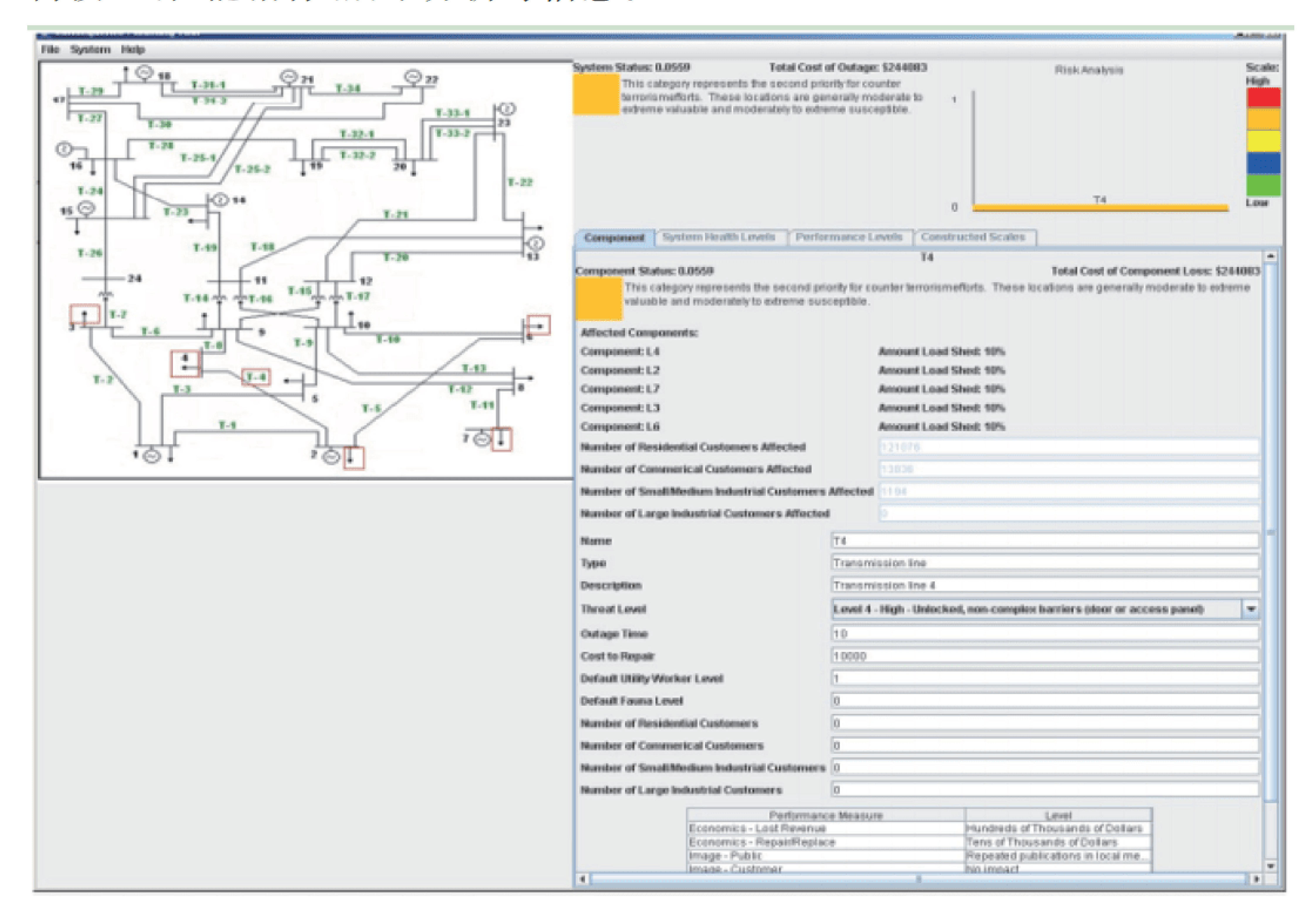


图 3-33　CMT 用户界面概览图(来源：文献[15] Figure 4)

在用户界面当中，可以对电力系统进行交互式可视化呈现，如图 3-34 所示。一方面，可以展现整体系统的拓扑结构，另一方面，可以对系统内的各组件状态进行监控。

该工具还支持对系统内各节点的状态进行如图 3-35 所示的设置，包括节点类型、威胁等级，在突发事件中，需要的备份时间、修复过程的成本、接入节点的用户类型及数量。通过这些设置，用户可以直观观察到：当某一节点遭受威胁或失效时，对整个系统和其他节点造成的影响、系统恢复时间及成本，以及可能的社会影响等信息。设置界面与分析报表见表 3-3。

3.3.4.3　系统脆弱性评估(system vulnerability assessments)

对 SCADA/EMS 系统的脆弱性评估，能够发现可能被利用的网络安全漏洞、可能允许未经授权的访问和关键数据窃取等漏洞。NSTB 系统脆弱性评估项目对控制系统中最具代表性的电力、石油和天然气行业进行评估，并促进新一代控制系统的研发，鼓励快速部署安全补丁，并指导设计未来系统和编码方式。

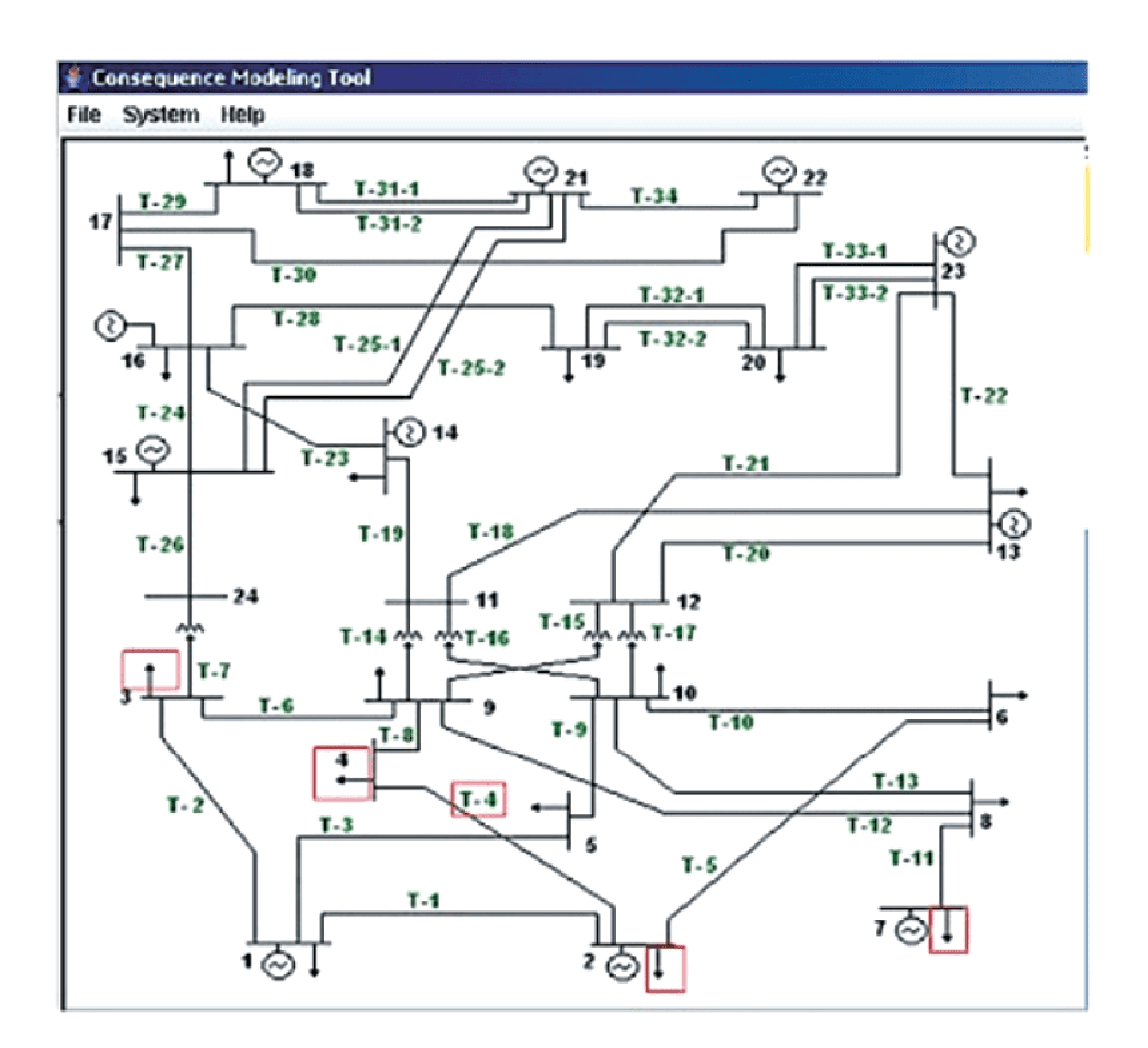


图 3-34　CMT 系统架构概览(来源：文献[15] Figure 5)

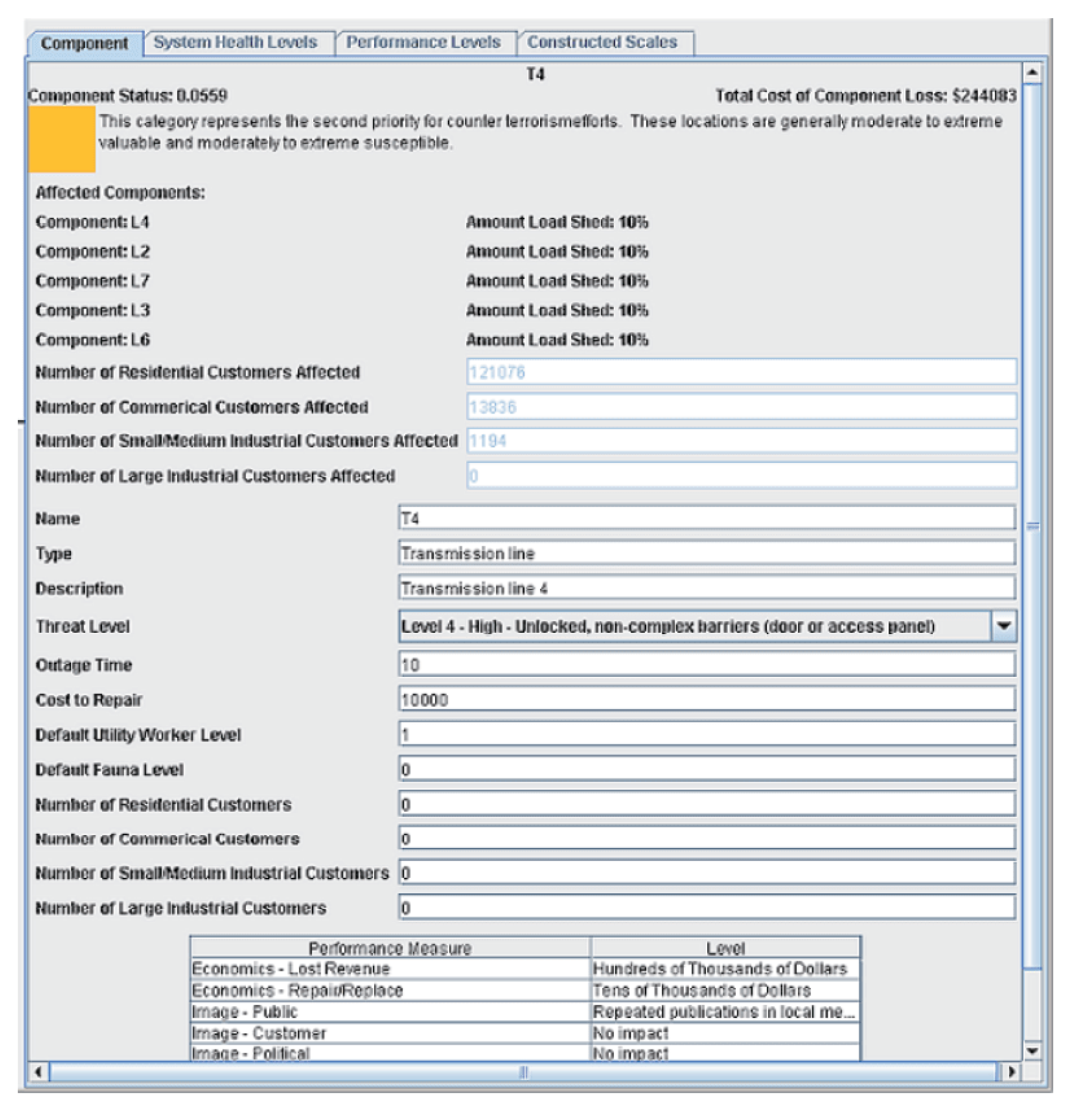


图 3-35　CMT 系统设置界面(来源：文献[15] Figure 6)

表 3-3 CMT 性能测试表

性能测试	等级
经济-代价收益	成百上千美元
经济-修复、替换	上万美元
图像-公开	在本地媒体重复公开传播
图像-客户	没有影响
图像-政治	没有影响
健康、安全-公共	没有影响
健康、安全-实用的工人	对于修复工作相关的工人有较低的安全影响
环境	没有影响

1. 设计目标

系统脆弱性评估项目计划实现以下目标：

（1）对电力、石油和天然气行业中最具代表性的 12 个工控系统进行评估，每年与产业合作进行三个系统的漏洞评估。每个评估将严格审查一系列能源部门的可能被利用和遭受网络攻击的潜在漏洞。评估工作完成后，评估报告提供给供应商，基于此信息来实现补丁修复，以及为系统用户提供升级加固服务。供应商也可以利用这些评估信息在未来系统设计中考虑进行安全设计。

（2）将控制系统网络安全评估功能转移到私营部门当中，逐步开展私营部门系统脆弱性评估活动。

2. 技术挑战和需求

缺乏工业方法和资源来检测和识别网络安全漏洞，这是能源行业面临的一个严重问题。增加企业网络和控制系统之间的连接网络，也可能在供应商和运营商的操作范围引入新的漏洞。快速发现控制系统漏洞，部署相关的安全补丁对于保护能源行业控制系统来说是至关重要的。

为应对这些挑战，系统脆弱性评估项目需要重点开展以下工作：

（1）设计脆弱性评估方法。

（2）识别最佳实践，减少能源控制系统漏洞。

（3）在不影响操作系统性能前提下，研究缓解系统漏洞的措施。

（4）NSTB 项目参与者、测试设备供应商和资产所有者相互合作，共同开展关键基础设施网络安全漏洞发现与修复工作。

3. 项目里程碑

图 3-36 中的 7 个里程碑事件的含义分别如下：

（1）评估应用于电力、石油和天然气的最具有代表性的 3 种工业控制系统控制系统，其中，电力行业系统包括电力变电站。

（2）开始启动将控制系统网络安全评估工作推广到私营部门的工作。

（3）利用 NSTB 资源，资助工业界主导两个典型系统的脆弱性评估工作。

（4）将一部分 SCADA NSTB 的测试资源开放给学术研究者、制造商和用户。

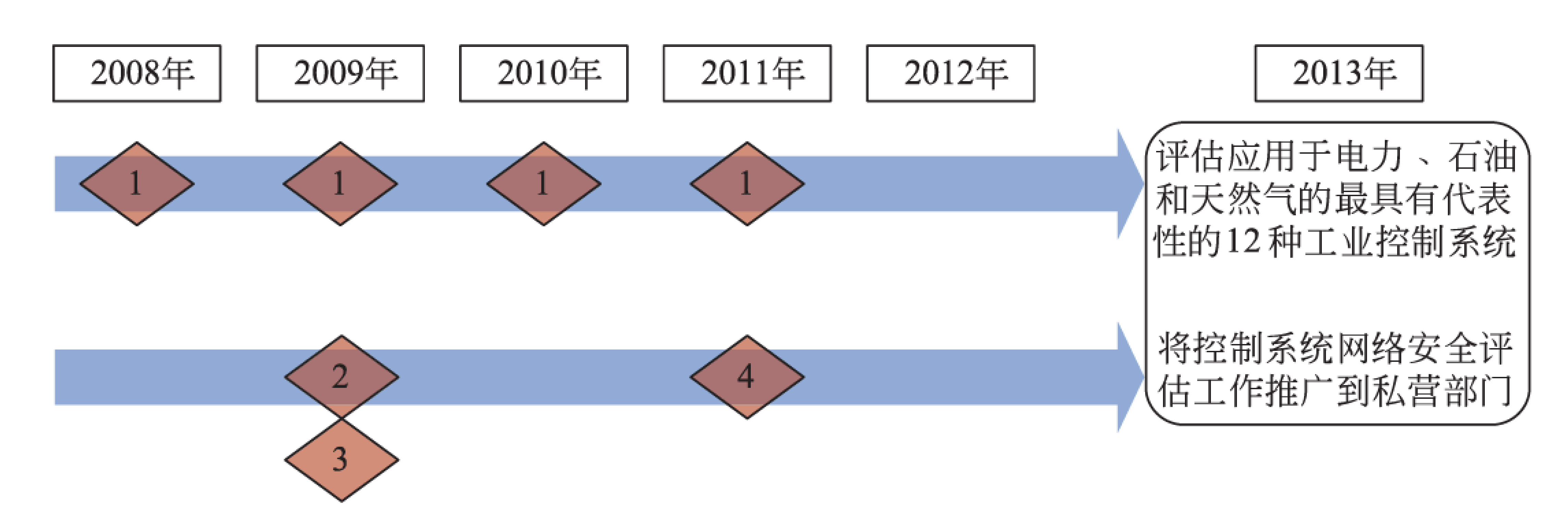


图 3-36　系统脆弱性评估项目里程碑

根据系统脆弱性评估项目的目标，本项目实施过程中在各财年设立了如下里程碑目标：

（1）2008—2011 财年：每年对 3 个最有代表性的，可用于电力、石油和天然气工业（包括变电站）的工业控制系统进行评估。

（2）2009 财年：将系统脆弱性评估项目转移到私营部门进行，利用 NSTB 的资源，对工业进行支持，对两个系统进行脆弱性评估。

（3）2011 财年：将 NSTB 的部分可用资源开放给研究人员、供应商和用户。

4. 主要项目

（1）常见系统漏洞分析[16]

① 项目目标

在与能源行业相关的工业控制系统当中存在一些脆弱性或漏洞问题，针对这些问题，该项目旨在为政府及能源行业提供安全解决方案。

② 普遍脆弱性评分系统（Common Vulnerability Scoring System，CVSS）

在 SCADA 系统中最重要的漏洞是那些未经授权的对物理系统的访问控制漏洞。SCADA 系统中较为脆弱的可用性和功能也可能对控制系统和基础设施管理产生重大影响。对 SCADA 系统的评估使用普遍脆弱性评分系统（CVSS）。CVSS 提供了一种包括 CVSS 基础测量、暂态测量和环境测量的标准评估方法。

通过如表 3-4 所示的 CVSS 基础测量，安全软件开发和系统管理可以减少 SCADA 系统漏洞的数量，在设计和实施监控产品过程中，遵循“最小特权原则”，评估脆弱性严重程度。

表 3-4 CVSS 基础测量表

基本特征	评估准则	等级
访问向量	脆弱性是如何被利用的	攻击者远程攻击主机的能力越容易，那么系统就越脆弱
访问复杂度	当攻击者获得了目标系统的访问权限后，攻击者利用系统脆弱性来实施攻击的复杂度	攻击者实施攻击的复杂度越低，那么说明系统的脆弱性问题越严重
身份认证	攻击者要想攻击成功一个目标系统，所需要经过的身份认证次数	如果攻击者攻击一个系统的过程中，所需要的身份认证次数越少，那么说明系统越脆弱
机密性影响	数据的机密性对于成功利用系统脆弱性来实施攻击的影响	如果系统的机密性问题对于攻击者实施攻击的影响越大，那么说明系统越脆弱
数据完整性影响	数据的完整性对于成功利用系统脆弱性来实施攻击的影响	如果系统的完整性问题对于攻击者实施攻击的影响越大，那么说明系统越脆弱
可用性影响	数据的可用性对于成功利用系统脆弱性来实施攻击的影响	如果系统的可用性问题对于攻击者实施攻击的影响越大，那么说明系统越脆弱

与基础测量一样，如表 3-5 所示的暂态测量，直接对系统漏洞进行评估，但这种测量侧重于监测随着时间变化的属性，并据此提供漏洞修复技术。

在不同的环境中的相同的漏洞对 SCADA 系统构成的风险也可能不同。如表 3-6 所示的环境测量对 SCADA 系统进行评估。这些指标反映了其在不同环境中受影响的组件的重要性。

表 3-5　CVSS 暂态测量表

暂态特征	评估准则	等级
利用性	当前系统状态可被利用性或代码可用性	一个脆弱性越容易被利用，那么系统就越脆弱
修复等级	可修复的等级	一个脆弱性问题越不容易修复，那么就说明系统脆弱性问题越严重
技术报告的机密性	脆弱性问题在现有技术报告中的存在性或者问题的描述详细程度	一个脆弱性问题越容易被制造商或其他渠道验证，那么这个脆弱问题越严重

表 3-6　CVSS 环境测量表

环境特征	评估准则	等级
并行破坏潜能	攻击破坏所带来的潜在的生命或设备财产损失	破坏所带来的损失越大，则系统脆弱性问题越严重
攻击目标分布性	存在脆弱问题的系统的比例	存在脆弱问题的系统越分布，那么脆弱性问题越严重
安全要求	受损的 IT 系统或设备对用户组织的重要性，一般是以数据的机密性、完整性和可用性来评估	系统对数据的机密性、完整性和可用性要求越高，那么脆弱问题越严重

③ 网络安全风险识别

NSTB 在改善操作系统和网络安全方面取得的显著成就包括：通过减少可用的端口和服务的数量来减少 SCADA 系统的主机暴露可能性；开发漏洞修复补丁；NSTB 利用 CVSS 评估了 SCADA 软件及生产设备，并分析了如表 3-7 所示的 10 种最关键的 ICS 脆弱性。

表 3-7　10 个最关键的 ICS 脆弱性

等级	影响、脆弱性	CVSS 脆弱性分数
1	最有可能访问、未打补丁的脆弱性问题	9.8
2	监督访问控制、使用脆弱性远程显示协议	9.8
3	监督控制访问、网页人机交互界面脆弱问题	9.8
4	工业控制系统主机访问、工业控制系统服务中的缓冲区溢出问题	9.3

续表

等级	影响、脆弱性	CVSS 脆弱性分数
5	工业控制系统主机访问、不恰当的身份认证问题	9.3
6	工业控制系统的应用访问、不恰当的访问控制或授权问题	9.1
7	工业控制系统身份认证凭证收集问题、使用明文数据来实现标准信息系统的身份认证协议	9.0
8	工业控制系统身份认证凭证收集问题、工业控制系统中传输层没有采取防护措施	9.0
9	监督访问控制、工业控制系统数据或命令遭受插入或篡改攻击问题	8.8
10	历史数据访问、SQL 注入攻击问题	8.6

CVSS 从多个漏洞数据库(如国家漏洞数据库)中的数据进行分析,并根据当前时间和特定环境确定漏洞的严重性及修复优先级。一般来说,在同样的基础和环境下,已知漏洞的优先级更高。表 3-8 总结了未修复的已公开系统脆弱性的安全特征。

表 3-8 未修复的已公开系统脆弱性的安全特征总结表

未修复的已公开系统脆弱性	
可能后果	工业控制系统主机或应用被攻击者劫持或捕获后,可能导致发生拒绝服务攻击、代码注入攻击、数据丢失或安全防护绕过等侧信道攻击
工业控制系统影响	对工业控制系统组件的未授权访问,最有可能的访问向量
脆弱组成部分	存在于主机上的未修复的操作系统,应用,服务和库
检测的难易程度	容易
攻击可察觉性	高
互联网攻击频率	高
修复代价	低
在工业控制系统中的存在广泛程度	高

远程显示协议和应用程序可用于远程访问,为远程机器提供登录和远程控制、图形显示功能。允许远程显示的应用程序和操作系统服务被广泛使用于

ICS 中，用于远程管理 ICS 主机或者对操作屏幕和其他 ICS 应用程序的访问。

用于 ICS 的远程显示协议存在一些漏洞包括：可接受来自任何地方的连接；证书使用明文传输；加密算法不够完整；即使使用强加密，如果远程显示端的主机被破坏，攻击者也可能由此访问远程 ICS 主机。

使用远程显示软件来对 ICS 进行远程访问和监控，这一行为可能成为 ICS 中最严重的漏洞。因为它可能允许远程用户在未经授权的情况下对图形监控软件以及其他功能进行远程访问。表 3-9 总结了远程显示协议的安全漏洞特征。

表 3-9　远程显示协议的安全特征总结表

远程显示协议的利用	
可能后果	可能导致拒绝服务攻击、代码注入攻击、数据丢失或安全防护绕过等
工业控制系统影响	未授权访问工业控制系统组件、未授权远程访问监控图形化软件，及其他可被远程控制的功能
脆弱组件	允许远程连接的工业控制系统主机及允许远程用户访问使用的应用
检测的难易程度	容易
攻击可察觉性	高
修复代价	低
在工业控制系统中的存在广泛程度	高

ICS 开发的网络服务往往容易受到攻击，攻击者可以利用 ICS Web 服务器获得未经授权的访问。系统架构经常使用网络隔离区保护关键系统并限制网络组件的开放。然而，ICS 中隔离区的 Web 服务器漏洞也可能通过允许访问外部边界，成为针对 ICS 攻击的突破口。并且，低安全水平的 Web 服务器可能会将更多的漏洞暴露给攻击者。表 3-10 给出了网页应用安全特征。

此外，本项目通过评估 ICS 安全风险发现，诸如较弱的认证以及会话跟踪、SQL 注入和跨站点脚本漏洞，都可能导致未经授权的用户对 Web 服务器和应用程序进行访问。同样地，Web 应用程序或服务器上的漏洞也可能会对物理系统产生风险。这些漏洞可能导致对图形监控软件的未经授权远程访问。此外，缓冲区溢出漏洞是最常见的输入验证缺陷类型漏洞，这往往是由程序员的失误造成的。利用缓冲区溢出，攻击者可能获得程序的特权，并利用代码创建交互式会话，以及发出命令。通过缓冲区溢出攻击进行远程代码执行是一种常见的攻击方法，进而在未经授权的情况下访问主机。表 3-11 给出了缓冲区溢出安全漏洞特征。

表 3-10 ICS 网页应用安全特征总结表

工业控制系统网页应用脆弱性	
可能后果	用户账号泄露或用户回话遭受劫持
	资源或功能暴露给非目标执行者，这可能会给攻击者提供敏感信息或给攻击者执行任意代码带来方便
工业控制系统影响	未授权访问网页人机交互界面，网页服务器或其他网页应用和功能，可能未授权远程访问到图形化监控软件，及其他集成到了网页应用中的功能
检测的难易程度	中到高
攻击者可察觉性	高
修复代价	低
在工业控制系统中存在广泛程度	高

表 3-11 缓冲区溢出特征总结表

工业控制系统服务中的缓冲区溢出问题	
可能后果	可能导致拒绝服务攻击、代码注入攻击、数据丢失或安全防护绕过等
工业控制系统影响	对工业控制系统组件的未授权访问，一般是发生在不同的安全区域
脆弱组件	发生在解析或接受解析网络流量的服务或其他应用中
检测的难易程度	容易
攻击者可察觉性	高
互联网攻击频率	高
修复代价	低
脆弱广泛存在程度	普遍存在
在工业控制系统中存在广泛程度	普遍存在

身份验证一般用于执行访问控制。较弱的身份验证可能会导致访问控制失灵。ICS 安全评估表明，针对处理数据和控制功能的访问控制都十分脆弱，它们不需要身份验证，或很容易进行规避。许多自定义的 ICS 应用程序使用了不当的身份验证，或根本没有任何身份验证机制。一个常见的错误是客户端身份验证，即只在本地客户端对用户进行身份验证。由于身份验证所需的信息同样存

储在客户端,攻击者很容易提取这些信息,或者修改客户端,以此规避身份验证。表 3-12 给出了不恰当的认证方式的安全特征。

表 3-12　ICS 应用中不恰当的认证方式

工业控制系统应用中身份认证不恰当	
可能后果	安全防护身份验证绕过
工业控制系统影响	对工业控制系统应用的未授权访问,对监控功能的未授权远程访问
脆弱组件	工业控制系统允许远程连接的主机和允许用户远程访问的应用
检测的难易程度	中
攻击者可察觉性	高
修复代价	低到高
攻击频率	有时
在工业控制系统中存在广泛程度	高

访问控制机制能够限制访问资源和服务的网络、主机和 ICS 的范围,操作者及使用条件。当账号、应用程序或主机受到攻击时,造成的影响取决于它们的特权等级。一旦攻击者获得了一台主机,便可以据此获得分区和访问控制权。一般情况下,一些设施被 ICS 默认作为根用户(组)进行服务。很多不必要的服务对此特权级别默认开放,这样做可能使系统资源暴露在本来可预防的风险之下。

在 ICS 的设计和实现中,一旦发现某些服务具有漏洞,通过对某些特权等级进行必要的限制,可以将攻击面以及遭受攻击的影响水平显著降低。服务的权限是通过用户的权利限制的。对任何服务的开发都可能让攻击者利用服务网络的权限来立足于 ICS 当中。攻击者还可能利用服务运行漏洞对自身特权进行升级,以获得更多的权限。一旦攻击成功,攻击者可以作为一个特权用户拥有对主机完全访问的权限。ICS 中不必要的功能、协议、服务和应用程序都会增加遭受攻击的可能,并增加后果的严重性。表 3-13 给出了不恰当的访问控制的安全漏洞特征。

表 3-13　不恰当的访问控制

工业控制系统应用中不恰当的访问控制	
可能后果	安全防护身份验证绕过,包括信息泄露、拒绝服务攻击,任意代码执行等
工业控制系统影响	对工业控制系统功能的未授权访问

续表

工业控制系统应用中不恰当的访问控制	
脆弱组件	工业控制系统网络,主机和功能
检测的难易程度	中
攻击者可察觉性	高
修复代价	低到高
攻击频率	经常
脆弱广泛存在程度	高
在工业控制系统中存在广泛程度	普遍存在

在 ICS 中,IT 系统的常见功能经常通过非加密的服务来实现。虽然已经拥有更安全的替代方案,这些不被使用的服务仍然存在于许多 ICS 中,并处于活跃状态。对 IT 协议进行明文身份验证,这一行为可能在传输过程中被攻击者嗅探到,并以此通过系统验证。如果攻击者能够获取用户名和密码,他能够合法登录到系统,并拥有用户特权。出于这个原因,纯文本远程登录服务应该替换为加密服务。使用不安全的协议和服务连接到 ICS 主机同样会在系统中创建一个高风险的访问路径。这是一个危险漏洞,因为它允许远程用户对 ICS 主机和功能进行未经授权的远程访问。表 3-14 总结了明文认证协议安全漏洞特征。

表 3-14 明文认证协议安全特征总结表

标准信息系统明文认证协议的使用	
可能后果	导致系统遭受身份哄骗攻击
工业控制系统影响	对工业控制系统组件的未授权访问:远程用户可以任何功能权限,进而可以远程访问主机
脆弱组件	工业控制系统中任何运行明文身份认证协议的主机
检测的难易程度	容易
攻击者可察觉性	高
修复代价	低
脆弱广泛存在程度	高
在工业控制系统中存在广泛程度	高

ICS 应用证书传输缺少保护的漏洞与“使用明文验证的标准 IT 协议”类似,均由于证书传输的保护缺失造成。在这种情况下,如果攻击者能够捕捉 ICS 应

用证书，他可以登录到 ICS 应用，并获得相关的 ICS 功能(可能包括控制物理过程，改变数据，或重新配置集成电路设备)。这一漏洞同样十分严重，因为它允许对 ICS 功能、人机界面应用程序(控制功能)的未经授权的远程访问。表 3-15 总结了应用中未经保护的用户凭证传输安全漏洞特征。

表 3-15　ICS 应用中未经保护的用户凭证传输

工业控制系统中未经保护的用户凭证传输	
可能后果	导致系统遭受身份哄骗攻击
工业控制系统影响	对工业控制系统应用的未授权访问:远程用户可以任何功能权限，进而可以远程访问监控控制功能
脆弱组件	工业控制系统应用
检测的难易程度	容易
攻击者可察觉性	高
修复代价	中
脆弱广泛存在程度	高
在工业控制系统中存在广泛程度	常见

ICS 网络协议，一般用于发送控制命令和状态数据。但是由于缺乏足够的访问控制和完整性检查机制，这些协议可能遭受篡改、重放和哄骗攻击。这一漏洞会暴露给拥有监控网络，或者设备控制网络访问权限的任何人。ICS 网络协议漏洞对物理系统可能造成的后果与远程显示协议漏洞和网络人机交互插件漏洞类似，因为它同样是通过监控网络进行攻击。

表 3-16 总结了 ICS 网络协议安全漏洞特征。

表 3-16　ICS 网络协议安全特征总结表

工业控制系统数据和命令遭受篡改和注入	
可能后果	数据泄露、篡改或丢失
	将数据或功能暴露给无意的执行者，这将可能给攻击者提供一些敏感信息或允许其执行恶意代码
工业控制系统影响	未授权访问网络级监控控制功能
脆弱组件	工业控制系统通信信道，以及不同安全区域之间可能被攻击者利用的区域
检测的难易程度	中到高
攻击者可察觉性	高
修复代价	高
在工业控制系统中存在广泛程度	普遍存在

作为ICS的一部分,历史服务器通常用于数据归档和分析,一般位于隔离区或公司网络之中。对历史服务器的威胁包括侵入主机和数据破坏。ICS中的历史服务器通常利用常见的SQL服务器作为它的后端。历史数据往往可以通过自定义网络界面或应用程序查看。历史数据的客户端应用程序是高风险组件,因为这些软件常常可以架设在企业环境中,可以为攻击者提供一个ICS网络的突破口。另外,攻击者可以访问未经授权的信息,在某些情况下可能导致经济损失。历史数据库应用程序通常使用SQL查询来检索信息。当应用程序对用户输入的过滤不足或错误时,便会产生SQL注入漏洞。如果攻击者将转义字符插入数据库查询,他们便可能获得对数据库任意读取或写入的权限。攻击者也可以修改SQL查询的逻辑安全控制(如身份验证)绕过安全验证。表3-17总结了ICS中SQL注入安全漏洞特征。

表3-17 SQL注入特征总结表

SQL注入	
可能后果	数据丢失:攻击者对数据库进行未授权读或写操作 绕过安全防护措施:针对数据库的拒绝服务攻击或者对相关主机实施未授权访问
工业控制系统影响	历史数据泄露,丢失或篡改是攻击者攻击工业控制系统的一条途径
脆弱组件	历史或其他数据库和主机,给予数据库的网页应用
检测的难易程度	容易
攻击者可察觉性	高
攻击者攻击频率	经常
修复代价	低
脆弱广泛存在程度	高
在工业控制系统中存在广泛程度	常见

④ 常见ICS漏洞分类

如图3-37所示,与通用的IT系统相比,工业控制系统的可用性的优先级最高,其次是完整性,最后是机密性。常见的SCADA漏洞可以根据不同的安全目标被分成不同类别。NSTB脆弱性评估过程的第一步是确定评估目标。由于接入点、过程、协议和设备一旦遭受破坏,便可能对控制系统产生严重的影响,所以它们被选定为评估目标。NSTB团队在脆弱性评估项目花费了900～1000小时以对选定的典型ICS中的评估目标进行测量评估。

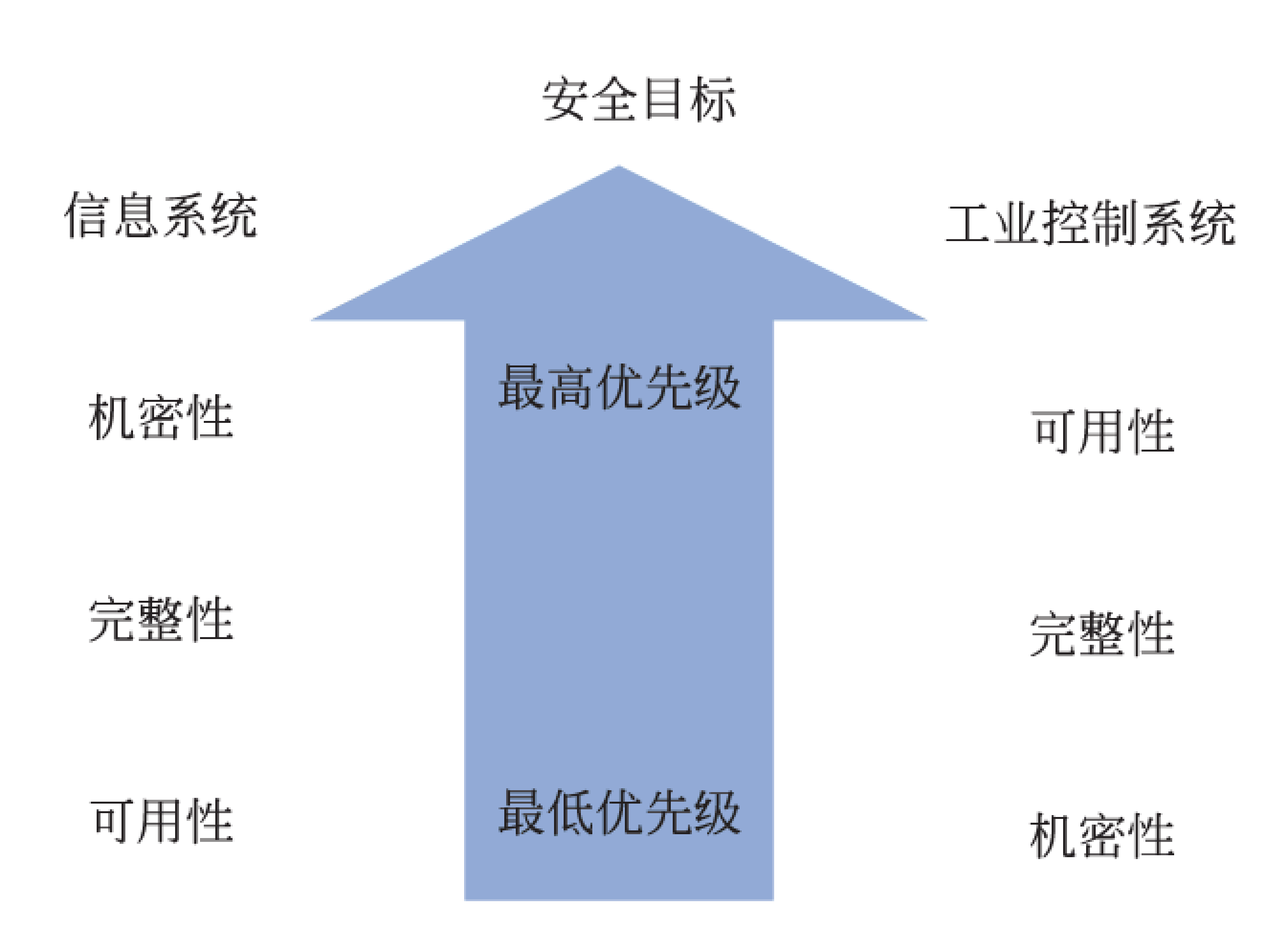


图 3-37 通用的 IT 安全目标与 ICS 安全目标对比图

由于选定的工控 SCADA 系统数量有限，对常见 ICS 漏洞的分类只能反映出真实环境下的大致情况。在研究过程中，研究团队将 SCADA 系统分为过程设备、过程控制硬件、网络设备和计算机部分，并将 SCADA 组件产品分为软件、硬件、固件和支持监控和数据采集的网络设备。

研究系统漏洞的发生频率也是很有意义的。这项研究可以在风险识别的基础上判断出系统更容易遭受哪一类安全攻击，以此判断系统的各个漏洞的权重。例如，系统可能遭受 50 次缓冲区溢出攻击，代表 50 个攻击向量；而只遭受一次身份验证攻击，但在风险识别当中分别只被算作一个漏洞，因而会对漏洞的危险等级进行误判。

此外，本项目还对各项漏洞对系统的影响进行了评估。例如，在 SCADA 系统当中的一个通信信道漏洞可能会影响到整个系统。

在漏洞类型方面，NSTB 评估团队分析了 SCADA 漏洞类型，分析了各种漏洞发生的可能性，得到了如图 3-38 所示的统计结果。此外，NSTB 评估团队还分析了这些漏洞被利用后，攻击者是否可以访问到 SCADA 系统的核心功能，得到了表 3-18 可以访问到 SCADA 系统核心功能的系统脆弱性类型及相应的攻

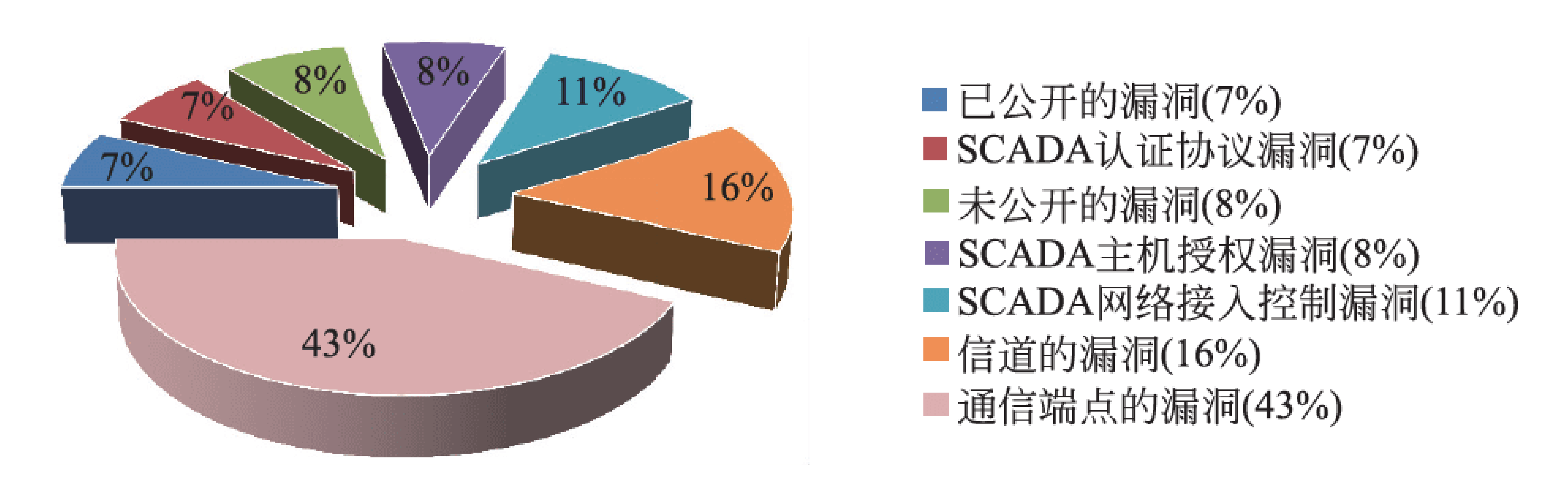


图 3-38 NSTB 评估安全脆弱性类型所占百分比的结果（来源：文献[16] Figure 4）

击目标所示的结果。

表 3-18 可以访问到 SCADA 系统核心功能的系统脆弱性类型及相应的攻击目标

脆弱类型	评估目标类别	脆弱性来源
已知脆弱性	最优可能实施攻击的路径	集成到 SCADA 产品中的未经修复的或老版本的第三方应用
		在 SCADA 主机上运行着的未经修复的操作系统
未公开的脆弱性	潜在的 0-day 漏洞或未经修复的脆弱性问题	由于开启了不必需的服务，导致大量的 SCADA 主机暴露在互联网上
		不恰当的 SCADA 代码
通信信道脆弱性	通过存在脆弱性问题的通信信道来对 SCADA 功能进行未授权访问	远程访问协议存在的脆弱性来源于哄骗攻击或中间人攻击
		SCADA 协议脆弱性的脆弱性来源于哄骗攻击或中间人攻击
通信中断脆弱性	对 SCADA 主机或应用的未授权访问攻击或拒绝服务攻击	SCADA 通信和数据传输协议的脆弱性服务
		数据库脆弱性
		网页脆弱性
SCADA 应用认证协议的脆弱性	通过利用认证机制的脆弱性来访问 SCADA 应用	认证机制绕过
		认证凭证管理
SCADA 主机授权脆弱性	一个 SCADA 账号所带来的破坏能力	对主机环境的安全防护失效
SCADA 网络脆弱性	通过可用的网络路径来对 SCADA 主机和功能进行访问	不恰当的网络设计
		不严谨的防火墙过滤规则
		对于网络设备的安全防护失效
		不恰当的网络监控

SCADA 系统漏洞可能允许攻击者在 SCADA 组件产品中收集信息，破坏或操纵 SCADA 操作。NSTB 评估主要集中在 SCADA 组件产品，以此来对漏洞的特征进行分类，并评估它们的设计和操作方式、对主机的影响和对网络安全的需求。图 3-39 给出了 NSTB 评估 SCADA 组件的结果。

如图 3-40 所示，NSTB 通过 SCADA 组件功能对研究中发现的系统漏洞进行了评估和分类。这一研究集中于通过系统功能受损这一结果，对系统漏洞进

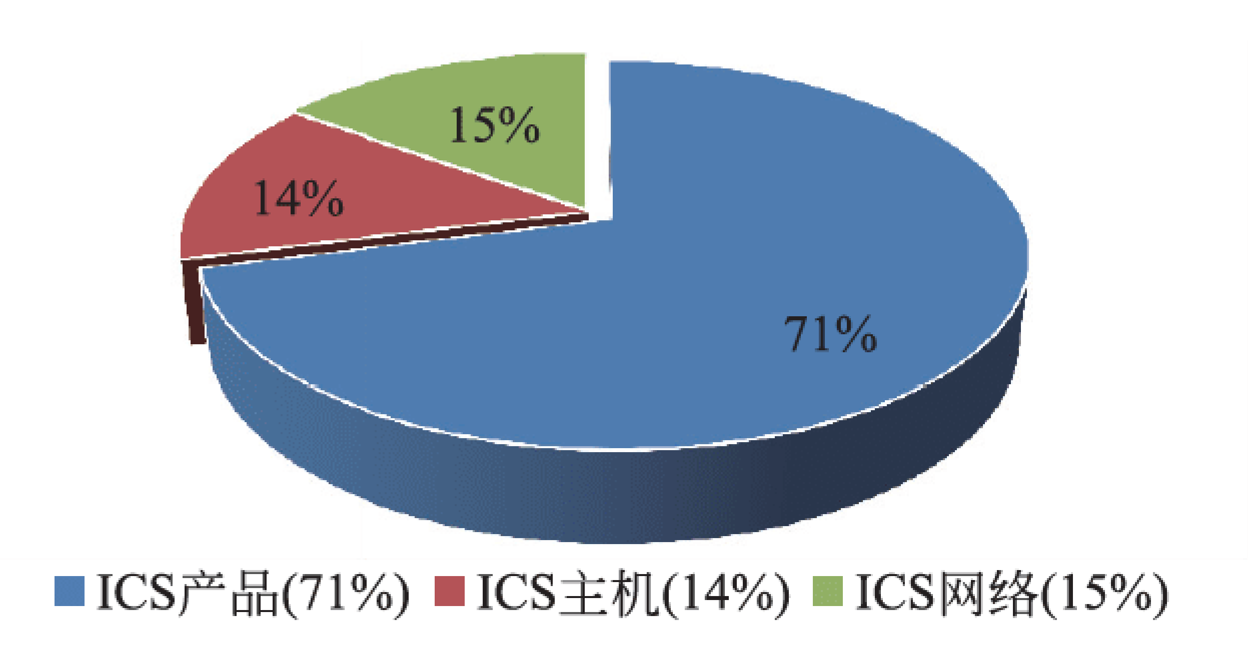


图 3-39　NSTB 测试发现的 SCADA 组件类别百分比结果(来源：文献[16] Figure 5)

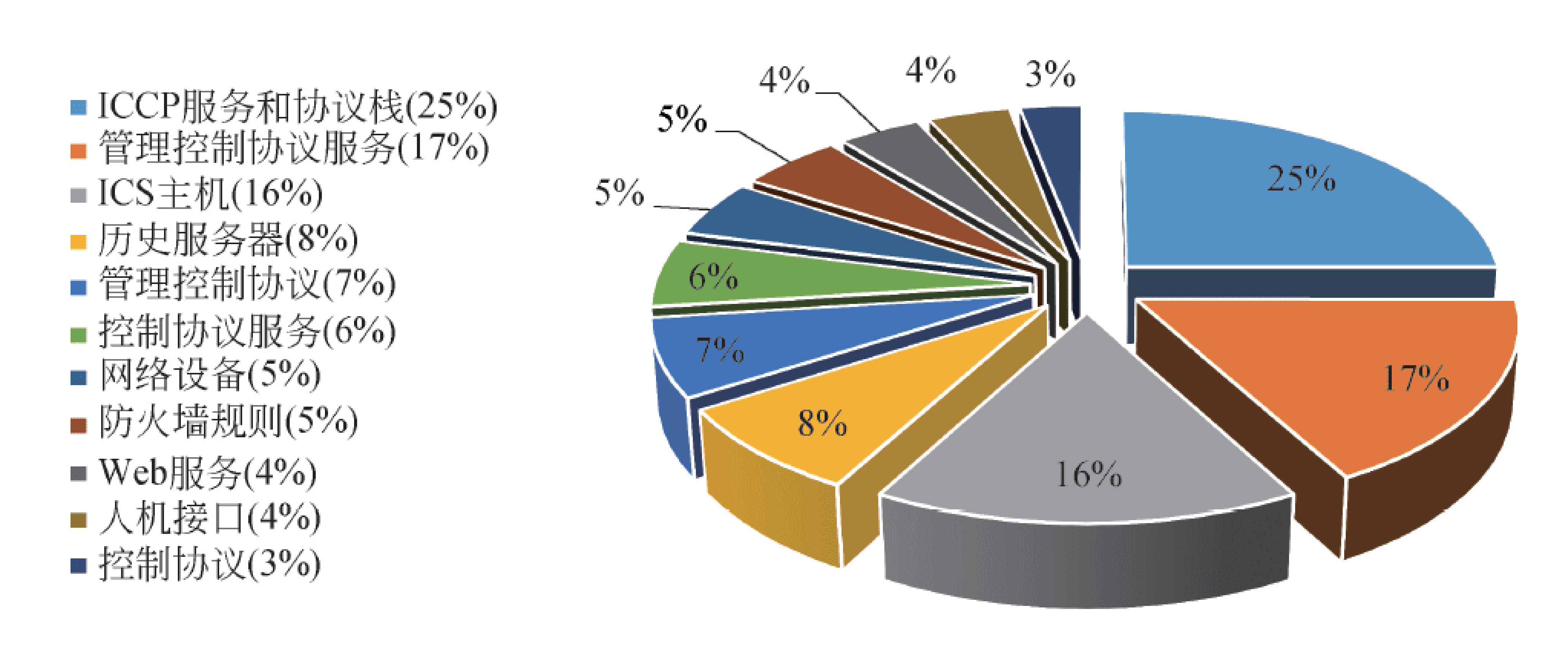


图 3-40　NSTB 测试分析得到的组件功能百分比结果(来源：文献[16] Figure 6)

行分类,并对在 NSTB 评估中发现的存在于 SCADA 服务器应用程序及服务中发生频率较高的漏洞进行分类说明。

几乎所有的 NSTB 评估当中,监督控制协议都是较为重要的一项。这一协议在 SCADA 系统中一般用于 SCADA 外部通信,由于其广泛的可用性,NSTB 评估将其放在一个较为重要的位置。内部控制中心通信协议(Inter-Control Center Protocol,ICCP)被选定为深入评估的协议。而一些评估系统并没有将“基本的”或“本地的”控制协议,如分布式网络协议(Distributed Network Protocol Version 3,DNP3),纳入评估指标。

通过使用图 3-41 所示的 ISA99 参考模型,NSTB 对出现在 SCADA 各架构层次上的漏洞进行了评估和分类。这个模型描述了 SCADA 系统的一系列基于功能的逻辑水平,对于建立漏洞分类参照系有很大作用。NSTB 的关注重点放在了核心 SCADA 功能上。如图 3-42 所示,NSTB 的研究表明,最有可能出现漏洞、遭受攻击的 SCADA 设施为监控与运营管理类设施。

⑤ SCADA 网络安全风险规避

安全活动的最终目的是为了降低风险。商业风险具有威胁、影响/后果和脆弱性的属性。如果网络威胁成功利用了脆弱性,商业风险就可能发生。为此,

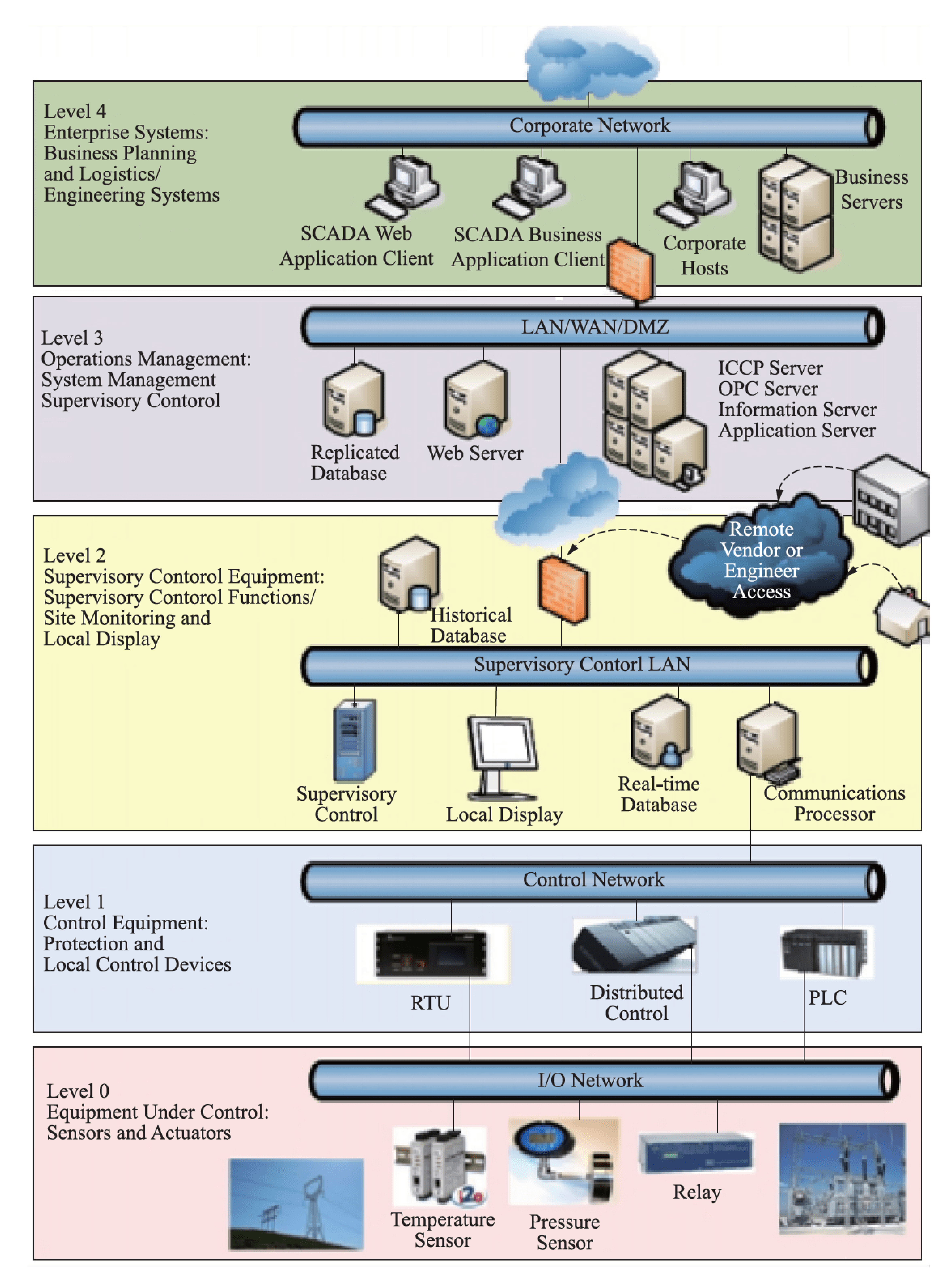


图 3-41 ISA SCADA 架构(来源:文献[16] Figure 8)

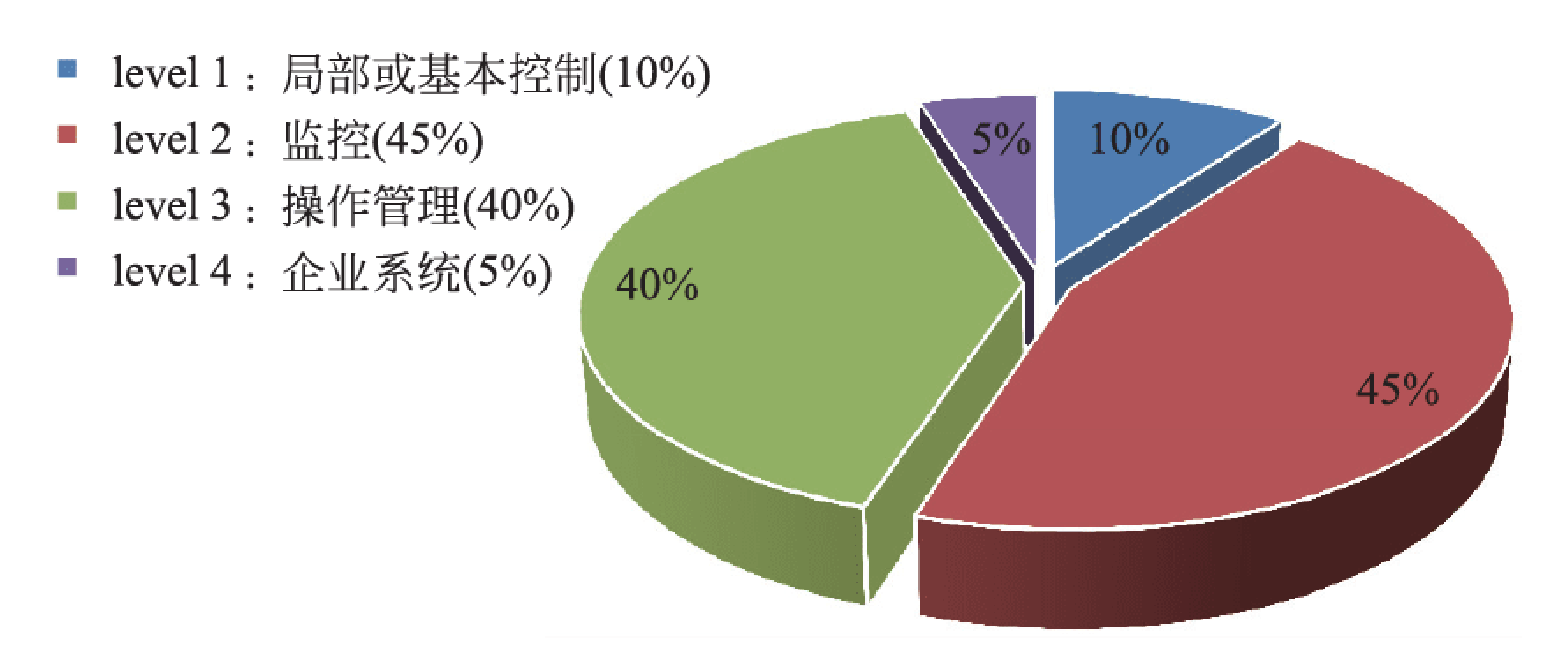


图 3-42　NSTB 测试得到的 ICS 功能级别结果(来源：文献[16] Figure 7)

CVSS 漏洞分析师提供了一个定性分析工具,以便供应商和用户控制系统来描述他们的网络安全风险。并为 SCADA 供应商和业主提供降低他们产品的 CVSS 评分的建议及例子。

经过表 3-19 和表 3-20 的分析测量,NSTB 提供了一系列可有效缓解系统脆弱性的方式:

表 3-19　SCADA 制造商减少系统脆弱性的措施

CVSS 特征	可以降低 CVSS 评分的措施
基准	• 安全开发实践 • 对所有用户和服务/应用实行最小权限 • 利用通用技术来测试软件的脆弱性,并进行修复
暂时修复等级	• 迅速测试第三方的补丁 • 在产品和服务生命周期内提供公开的漏洞报告 • 迅速的补丁修复 • 产品和技术支持使用强认证和加密机制 • 提供适用于 SCADA 组件和制定 IDS 规则的详尽的产品或技术文档

表 3-20　SCADA 拥有者减少系统脆弱性的措施

CVSS 特征	可以降低 CVSS 评分的措施
暂时修复等级	• 关注用户和制造商对于脆弱性漏洞的反馈和发布 • 迅速的补丁修复 • 识别并开展解决方案来修复系统脆弱性 • 使用并支持强认证和加密机制 • 保护关键功能 • 常见和开展特定的防火墙和入侵检测规则 • 紧密关注关键功能和安全日志来标定正常和异常行为

(1) 通过去除所有不需要的应用程序和有效的补丁管理来缓解固有漏洞。

(2) 通过身份验证凭据保护减轻传输通信信道的漏洞,确保本地和远程访问控制和 SCADA 系统的数据完整性检查。

(3) 通过安全的编码实践缓解通信端点漏洞,加强 SCADA 和 ICCP 服务严格的输入数据验证,数据库应用程序和 Web 服务。

(4) 通过在服务器和客户端的身份验证,以及有效的身份验证凭据的有效管理,减少身份认证方面的安全漏洞。

(5) 通过最小权限的访问控制功能,缓解授权漏洞。

(6) 通过网络分割、强大的防火墙规则、安全连接的安全区和入侵检测来缓解网络接入漏洞。

(7) 保护攻击面。攻击面包括攻击系统的所有可能的途径。一个系统的攻击面包含一组方法,攻击者可以进入系统,并有可能造成损害。因此,攻击面越小,系统也就更安全。NSTB 提出了几项对攻击面防护的策略,包括:设计并实现安全的代码,用安全的代码替换可能遭受攻击的代码,验证输入数据,防止缓冲区溢出,防止 SQL 注入,防止跨站点脚本,防止目录遍历,最小化端口和服务,确定必要的端口和服务。

安全的编码资源可用于所有应用程序类型和语言。为此,表 3-21 列举了所有最常见的 SCADA 编程错误。

表 3-21 常见 SCADA 编程错误

脆弱性分类	常见脆弱问题
数据处理	不恰当的语法结构处理
	不恰当的数据值处理
	不恰当的丢失数据处理
	不恰当的输入验证
	不恰当的编码或输出溢出
	有符号到无符号数据转换错误
	不正确的字节顺序
缓冲区溢出限制边界错误	缓冲区复制时没有检查输入大小
	基于数据栈的缓冲区溢出
	基于堆的缓冲区溢出
	越界访问
	不恰当的数组索引验证
	不正确的缓冲区大小计算

续表

脆弱性分类	常见脆弱问题
缓冲区溢出限制边界错误	不恰当的终止条件
	整数溢出
	整数溢出到缓冲区溢出
不良代码质量标志	可信变量或数据存储的外部初始化
	初始化缺失
	使用未经初始化的变量
	空指针
	不受控制的资源消耗(死循环)
	未经验证的返回值
	未经验证的返回值到一个空指针
	在执行完后,未采取释放内存操作
网页问题	不恰当的路径名限制
	保存网页结构失败
	保存 SQL 查询结构失败
异常情况处理失败	句柄丢失
	未捕获异常情况
	不恰当的异常情况处理
	未采取行动的错误异常检测

3.4　小结

美国能源部主要关注能源行业,负责制定能源领域的战略规划,管理能源行业发展,主导研发能源领域相关技术等。本章首先介绍了美国能源部管辖的国家实验室的基本情况,然后介绍了美国能源部为了应对能源领域关键基础设施网络安全问题制定的安全防护技术路线报告,以及著名的国家 SCADA 测试床项目情况。

通过分析可知,美国能源部在能源领域不仅积累了雄厚的科研基础和丰富的实践经验,而且还通过统一规划和管理的方式搭建了国家级测试床,以此来整合全国各大实验室的科研资源,帮助相关人员开展风险和脆弱性评估工作,进而更有效地研发下一代控制系统。

参考文献

[1] USDepartment of Energy. Office of Science. The DOE Laboratory System. http://science.energy.gov/laboratories/

[2] US Department of Energy. Office of Electricity Delivery & Energy Reliability. National SCADA Test Bed. http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed

[3] Eisenhauer. Roadmap to secure control systems in the energy sector. Energetics Incorporated. Sponsored by the US Department of Energy and the US Department of Homeland Security 2006.

[4] US Department of Energy. Roadmap to achieve energy delivery systems cybersecurity. https://energy.gov/oe/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011

[5] US Department of Energy. DOE/OE National SCADA Test Bed Fiscal Year 2009 Work Plan. https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/FY09_Work_Plan_External.pdf

[6] US Department of Energy. National SCADA Test Bed Program Multi-Year Plan FY2008-2013. https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_OE_NSTB_Multi-Year_Plan.pdf

[7] Idaho National Laboratory. Idaho's test range-fact sheets. https://factsheets.inl.gov/FactSheets/idaho-test-range.pdf. 2005

[8] Idaho National Laboratory. Idaho's test range. https://factsheets.inl.gov/SitePages/NationalAnd Homeland SecurityFactSheets.aspx

[9] DHS. LOGIIC cyber security system brochure. https://www.dhs.gov/publication/csd-logiic-brochure

[10] US Department of Energy. Secure data transfer guidance for industrial control and SCADA Systems. http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf

[11] Pacific Northwest National Laboratory. GridOPTICS™ power networking，equipment，and technology (powerNET) Testbed. http://gridoptics.org/docs/FPGI-FA1-edgar.pdf

[12] Alfonso Valdes. Detection and analysis of threats to the energy sector：DATES. http://www.osti.gov/scitech/servlets/purl/1010661

[13] Dong Wei，Yan Lu，Mohsen Jafari，et al. Protecting intelligent distributed power grids against cyber attacks. http://www.osti.gov/scitech/servlets/purl/1033753

[14] Michael J，McDonald et al. Modeling and simulation for cyber physical system security research development and applications. http://prod.sandia.gov/techlib/access-control.cgi/2010/100568.pdf

[15] Bryan T. Richardson, Lozanne Chavez. National SCADA test bed consequence modeling tool. http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/29-Consequence_Modeling_Tool_Report.pdf
[16] Idaho National Laboratory. NSTB assessments summary report common industrial control system cyber security weaknesses. https://www.fas.org/sgp/eprint/nstb.pdf

第 4 章　美国国家标准与技术研究院

4.1　国家标准与技术研究院及典型项目简介

隶属于美国商务部的美国国家标准与技术研究院(National Institute of Standards and Technology,NIST)创建于 1901 年,是美国历史最悠久的物理科学实验室之一。NIST 的主要职责就是在智能电网、电子健康记录、先进纳米材料,计算机芯片、技术、测量等方面制定标准规范。

在工业控制系统信息安全方面,NIST 于 2010 年 10 月发布了 SP 800-82《工业控制系统(ICS)安全指南》[1],它是依据 2002 年《联邦信息安全管理法》、2003 年国土安全总统令《第 7 号国土安全总统令:关键基础设施识别、优先级排序和保护》(Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection)等文件编制而成。在国家基础设施安全防护方面,NIST 于 2014 年发布了《改进关键基础设施网络安全的框架》第一版[2],这是美国政府首次对国家关键基础设施提出的安全标准。

此外,在具体的工控领域,NIST 主要在智能制造、智能电网、智慧城市、信息物理系统及公共安全通信等领域以及工业控制系统网络安全性能测试床方面都部署了相应的项目,开展了一系列研究工作。

1. 智能制造系统的网络安全

智能制造系统需要防范由于互联互通、使用无线网络和传感器以及采用常见信息技术所引入的潜在安全威胁和安全漏洞。智能制造系统的网络安全项目[2]将制定出一个包含指导方针、方法、指标和工具的网络安全风险管理框架。对于采用了网络安全技术的智能制造系统,该框架可以帮助制造商、技术提供商和解决方案供应商来评估系统在安全性能和可靠性方面是否达标。网络安全风险管理框架与具体的方法、指标和工具可有效地促进制造商采用安全技术,以此来实现一个安全、可靠、可持续运行的弹性智能制造系统。

由于早期部署到制造系统的传统 IT 安全措施会影响制造系统的实时性、资

源使用、操作可靠性和效率，因此，智能制造业系统的网络安全亟须新的技术理念来提供适用于制造系统的解决方案。该项目分成评估、测试开发和标准化三个实施阶段。

在评估阶段，NIST 将举办关于网络安全对系统影响的研讨会，定量地确定网络安全对智能制造系统的实时性、资源使用、可靠性和安全性的影响。

在测试开发阶段将解决两个研究挑战。第一个挑战是提炼总体需求，并归纳复杂智能制造系统实际的、可互操作的网络安全应用案例。第二个挑战是，针对这些需求和应用案例，开发一套网络安全技术测试集。该项目将开发智能制造系统网络安全测试平台，在此平台上执行制定的测试集，并分析安全技术对系统运行性能的影响（如延迟、抖动）和业务操作的影响（如效率、生产力）。基于测试结果，NIST 将整体出详细的技术分析报告。

在标准化阶段，NIST 将与国际自动化学会（International Society of Automation，ISA）和国际电工委员会（International Electrotechnical Commission，IEC）等标准化组织一起，合作制定新的指导方针和标准。这些新的指导方针和标准，将在不对智能制造系统的系统性能产生负面影响的前提下，设计实施网络安全防护措施。NIST 将确保新标准易于进行合规性测试。NIST 将与 ISA 的安全合规性协会（Security Compliance Institute，ISCI）合作开发用于为工业自动化供应商和运营者提供资格认证和测试方法的网站。通过与 ISCI 合作，NIST 希望确保本项目的最终成果可在智能制造业领域获得广泛推广和应用。

2. 智能电网的网络安全

由 NIST 的信息技术实验室（Information Technology Laboratory，ITL）和计算机安全部门联合管理的智能电网互操作性专家咨询小组（Smart Grid Interoperability Panel，SGIP）网络安全委员会（Cybersecurity Committee，CC），在智能电网领域，于 2014 年发起了智能电网网络安全项目[4]。该项目不仅要应对敌手的蓄意攻击，如来自心存不满的内部员工、工业间谍和恐怖分子的攻击，也需要应对由用户操作失误、设备控制失效、自然灾害所导致的信息基础设施故障。具体地，该项目主要目标是制定高级电表架构（Advanced Metering Infrastructure，AMI）的安全要求、云计算、供应链和隐私保护等相关标准。该项目旨在为智能电网提供基础网络安全指导、网络安全审查的标准和要求，进而为智能电网系统互联互通和跨部门网络安全协同响应提供指导建议。智能电网网络安全项目的主要目的是，促进智能电网网络安全技术标准化工作，具体技术包

括隐私保护、安全政策、安全响应流程和应急恢复等。

当电网系统部署了新的智能电网技术后，电力行业面对着新的网络安全威胁。智能电网互操作性专家咨询小组网络安全委员会通过分析这些新的安全需求，制定网络安全政策，编制智能电网网络安全方面的有关指导文件。本项目通过以下方式来开展研究：

（1）SGCC 提供网络安全专业知识和技术指导。

（2）SGCC 审查 NIST 跨部门报告(Interagency Report，IR)7628 第一版所确定的安全需求和智能电网互操作性要求的差距，对下一步工作提供建议。

（3）SGCC 领导 AMI 网络安全研发工作。SGCC 与 SGIP、电力科学院(Electric Power Research Institute，EPRI)、美国国家标准协会(American National Standards Institute，ANSI)等一起合作制定 ANSI C12.19 工业设施工业终端设备数据表的网络安全需求。此外，SGCC 还参与了巴西国家认可机构 INMETRO(The National Institute of Metrology，Standardization and Industrial Quality)制定 AMI 安全需求的项目。

（4）SGCC 将 NIST 制定的安全内容自动化协议(Security Content Automation Protocol，SCAP)进行扩展以支持智能电网系统。SGCC 拟研究并扩展美国能源部和电力科学院联合开展的 Lemnos 项目，旨在将安全内容自动化协议扩展应用到智能电网系统中，为智能电网组件提供标准的、可测量的自动监测安全分析功能，提高安全分析的精度和准确度，降低安全实践的成本，提高组件之间的安全互操作性。

（5）建立智能电网网络安全测试实验室。SGCC 建设了智能电网网络安全测试实验室以后，与 NIST 的信息技术实验室(Information Technology Laboratory，ITL)软件和系统部门一起研究、测试与 IEEE 1588 标准中关于电网系统时间同步问题。

（6）进一步细化并完善智能电网的安全架构、隐私保护和云服务等问题。

（7）培养供应链安全意识。SGCC 与能源部、联邦能源管理委员会(Federal Energy Regulatory Commission，FERC)、国土安全部及 SGCC 会员单位一起研究制定智能电网供应链安全指导方案。

本项目主要成果：

（1）NIST 发表了 NIST IR 7823 高级电表架构智能电表可升级性测试框架(Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework)草案。NIST IR 7823 草案提出了符合 AMI 智能电表固件升级过程要求一致性的测试实例。

(2) NIST 发表了 NIST IR 7628 智能电网网络安全指导(Guidelines for Smart Grid Cyber Security)的第一、二和三部分已经得到了美国基础设施制造商和管理者以及国际同行的广泛认可。NIST 已经完成了 NIST IR 的第一个版本,并征求了厂商和相关部门的意见。

3. 智慧城市的网络安全

目前,不同国家都在致力于利用信息物理系统(Cyber Physical Systems,CPS)和物联网技术来更好地管理城市资源,改进公共安全、健康卫生、教育、交通等社会服务,最终实现智慧城市的构想[5]。这个愿望能否实现,完全依赖于信息物理系统和物联网的安全问题是否能够得到妥善解决。NIST 在实现智慧城市的过程中,需要做到以下贡献:

(1) NIST 应该促进发展不同组织、部门之间的合作关系,以此来证实物联网和信息物理系统的确可以给美国带来有立竿见影的社会经济效益。这些效益包括提供就业机会,带来新的商机,提高经济增长速度,改善人民生活水平等。

(2) NIST 应该通过其在信息工程、信息和通信技术、材料科学和物理等方面的专业知识来为社会提供研究基础资源。

(3) NIST 需要为城市管理人员和物联网技术研发人员制定一个安全性能标准,提供测试工具及相关技术指导,帮助他们更好地设计和实现安全有效的智慧城市解决方案。

因此,NIST 建立了智慧城市的网络安全项目,本项目的主要目标包括:

(1) NIST 为智慧城市系统的设计和分析提供科学依据。

(2) NIST 协调组织不同单位一起制定智慧城市系统之间互操作性标准和指导文件。

(3) 通过推动智慧城市测试床的搭建工作来为实际系统的设计提供指导意见。

(4) NIST 要力争成为智慧城市解决方案的先锋力量。

其中,项目的目的是为可互操作、可复制和可扩展信息物理系统提供测试的科学依据和标准。进而使得这些系统能够更容易和高效地部署到城市中,提高运行效率、系统安全性、可恢复性和可持续性,提高人民的生活质量。

4. 信息物理系统的参考框架

信息物理系统(CPS)是一种集成了物理设备、计算设备和信息交互网络的新型智能系统。信息物理系统和相关的系统(如物联网系统、工业互联网系统

等)是被公认为有巨大发展和创新潜力的系统,这些系统将在多个领域影响世界经济和社会的发展。典型的应用领域包括能源基础设施、先进制造、楼宇控制、运输、医疗等。当前这些系统的设计和管理方法都是针对特定领域设计和制定的,其跨领域的通用性差。在不同领域应用时,这势必会带来许多额外的定制化工作。此外,目前的 CPS 在设计、评价和验证方面缺乏形式化分析方法。NIST CPS 的参考框架项目[6]通过统一通用词汇、分析方法和参考系统架构的方法来设计 CPS 框架,并且为各个领域的共同发展、信息交换提供了应用实例。通过提供跨领域的通用技术和基础理念,本项目旨在使 CPS 的设计、开发和运行更加安全、可靠。本项目还致力于通过由来自产业界、学术界和政府机构的技术专家所组成的 CPS 公开工作组(Cyber-Physical Systems Public Working Group, CPS PWG),促进公共部门和私营部门利益相关者之间的合作关系。本项目制定了以下研究计划:基于 NIST 的 CPS PWG 的成功开展和运行,起草一个 CPS 参考框架;评估 CPS 参考框架中的分析方法在不同应用领域的技术适用情况,调整修改在特定应用领域特定的词汇、分析和设计方法;通过分析利益相关者的反馈意见,不断细化、完善草案中的 CPS 参考框架;在国内和国际上,引进和对接与 CPS 参考框架相关的标准和技术。

4.2　提高关键基础设施网络安全的框架规范

在第 21 号总统令《提高关键基础设施的安全性和恢复力》的指导要求下,3000 多个信息安全专家在全国举办了一系列工业安全研讨会,共同讨论了 10 个月后,NIST 起草了《提高关键基础设施网络安全的框架规范》(简称规范)[2]的第一个版本。2014 年 2 月 12 号,美国白宫公布了这一规范。该规范不仅仅是信息安全新形势下,美国政府首次提出的国家级信息安全指导规范,而且还是自 2013 年美国启动了保护关键基础设施信息安全战略以来的第一个较全面的基础性指导文件。规范中制定的提高关键基础设施网络安全的框架是一个基于风险评估方法来管理网络安全风险的安全框架,包括框架核心、框架实现层级和框架配置文件,该框架可以帮助相关组织机构来识别安全风险、实施和改进网络安全实践。在该框架下,所涉及安全风险评估、处理及相关信息安全技术都要经历不断完善和更新。此外,制定者也会根据工业界的反馈来周期性地对框架进行修订。该框架提供了一种评定机制,该机制使得组织机构可以确定他们当前的网络安全能力,设定各自的安全目标,建立一个改进和完善网络安全防护系统的计划。该框架包括框架核心、框架实现等级和框架配置文件。

4.2.1 规范简介

为了应对关键基础设施所面临的信息安全风险，规范为风险管理者建立了基于风险评估的信息与决策流程模型。该模型从决策层、业务流程处理层和实现操作层三个层面上来协作处理安全风险事件。如图 4-1 所示，从安全事件生命周期的角度出发，规范设计的信息安全防护体系框架包括识别(identify)，保护(protect)，检测(detect)，响应(respond)和恢复(recover)五个方面。此外，规范还提供了一种网络安全水平评定机制，该机制有助于工控组织机构确定其当前的网络安全能力，设定各自的安全目标，建立一个改进和完善网络安全防护系统的计划。在该规范指导下，所涉及的安全风险评估、处理及相关信息安全技术都要经历不断完善和更新。制定者也会根据工业界的反馈来周期性地对框架进

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

图 4-1　信息安全防护体系框架(来源：文献[2] Table 1)

行修订完善。

在图 4-1 所示的框架中的五个方面的具体含义如下。

(1) 识别：对组织有重要业务关联的数据、人员、设备、系统和设施的识别和管理，使其对于业务目标的相对重要性与组织风险策略一致。

(2) 保护：制定和实施相关防护措施，确保关键基础设施运行安全。

(3) 检测：制定和实施相关措施，识别网络安全事件的发生。

(4) 响应：制定和实施相关措施，对检测到的网络安全事件采取响应行动。

(5) 恢复：制定和实施相关措施，保证网络安全事件发生后，关键基础设施具有一定的恢复能力。

4.2.2　框架核心

如图 4-2 和图 4-3 所示，框架核心是一个包括描述网络安全活动、安全预期产出和适用于关键基础设施领域不同行业的安全防护参考文献的集合。该框架核心为不同组织从决策层到实现操作层面的人员提供了可参考的工业标准、指导规范和安全实践等内容。具体地，该框架核心包含了关键基础设施安全风险评估与处理的五个环节，即识别、保护、检测、响应和恢复。它不仅完整地描述了安全风险的全生命周期，而且还针对每个环节细分后的子环节一一给出了对应的可参考文献(标准、指导规范或安全实践)。

Funcitions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

图 4-2　框架核心(来源：文献[2] Figure 1)

(1) 框架核心包括识别、保护、检测、响应和恢复五个重要安全“功能”。这五个功能是对网络安全提出的总体目标。

(2) “类”是根据不同的安全需求，对框架核心中的五个“功能”进行细分后

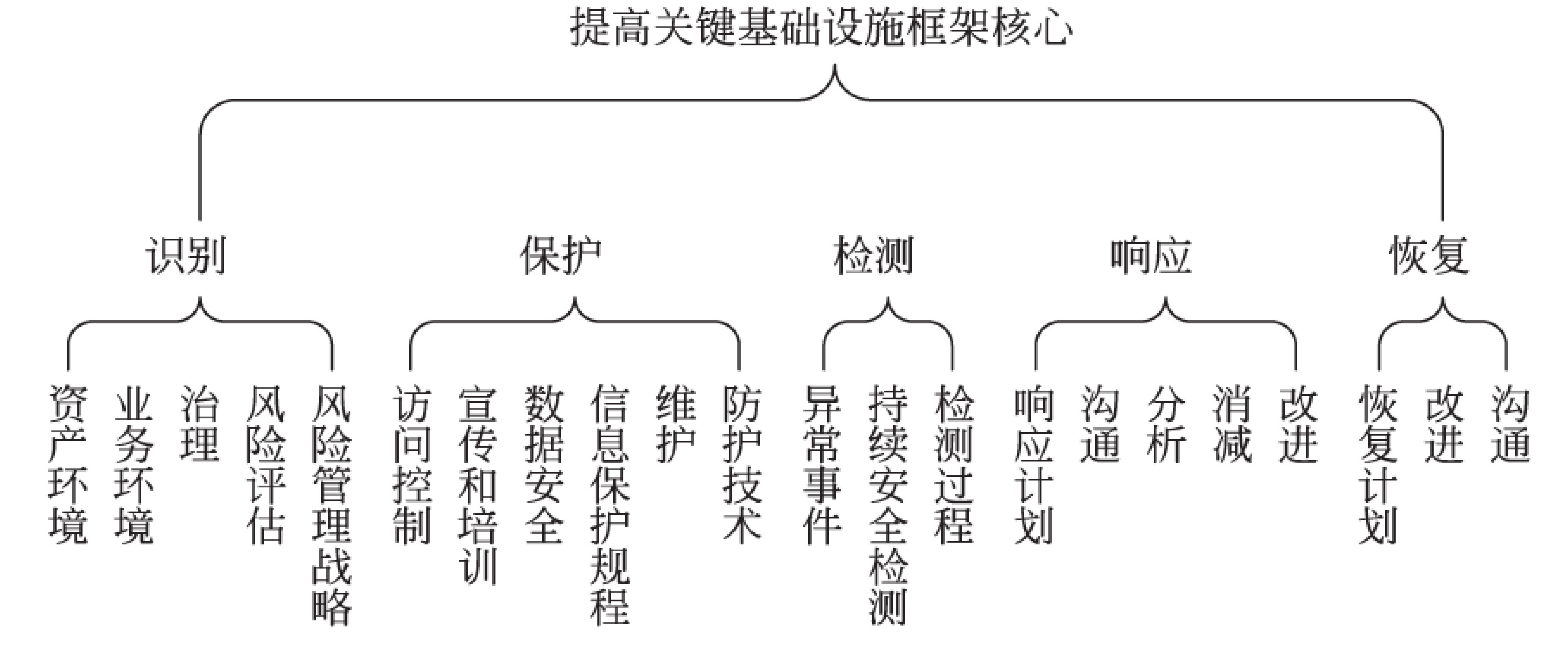


图 4-3　框架核心及其包含的类

的网络安全要素。

（3）“子类”是根据技术或管理活动，对“类”的进一步细化。图 4-4～图 4-8 分别给出了每一类所包含的子类。

- 识别
  - 资产管理
    - 组织内的物理设备和系统清单
    - 组织内的软件平台和应用清单
    - 组织内的通信和数据流拓扑图
    - 外部信息系统分类
    - 根据敏感度重要性和业务价值对资源进行优先级排序
    - 明确全体职工和第三方利益相关者的网络安全角色和职责
  - 业务环境
    - 确认和沟通组织在供应链中的作用
    - 确认和沟通组织在关键基础设施及其产业领域中的定位
    - 确认和沟通组织使命、目标和活动的优先级
    - 明确关键服务的附属和关键功能
    - 明确关键服务恢复能力的相关要求
  - 治理
    - 建立组织信息安全策略
    - 协调内部员工和外部合作伙伴之间的信息安全角色和职责
    - 制定网络安全法律、法规
    - 应对网络安全风险的治理和风险管理流程
  - 风险评估
    - 识别和记录资产漏洞
    - 从信息安全共享论坛接受威胁和漏洞信息
    - 识别和记录外部威胁
    - 识别潜在业务影响
    - 通过威胁、漏洞和影响来明确风险
    - 风险响应识别和排序
  - 风险管理战略
    - 建立风险管理流程
    - 明确和清晰描述组织风险承受力

图 4-4　识别功能及其包含的类和子类

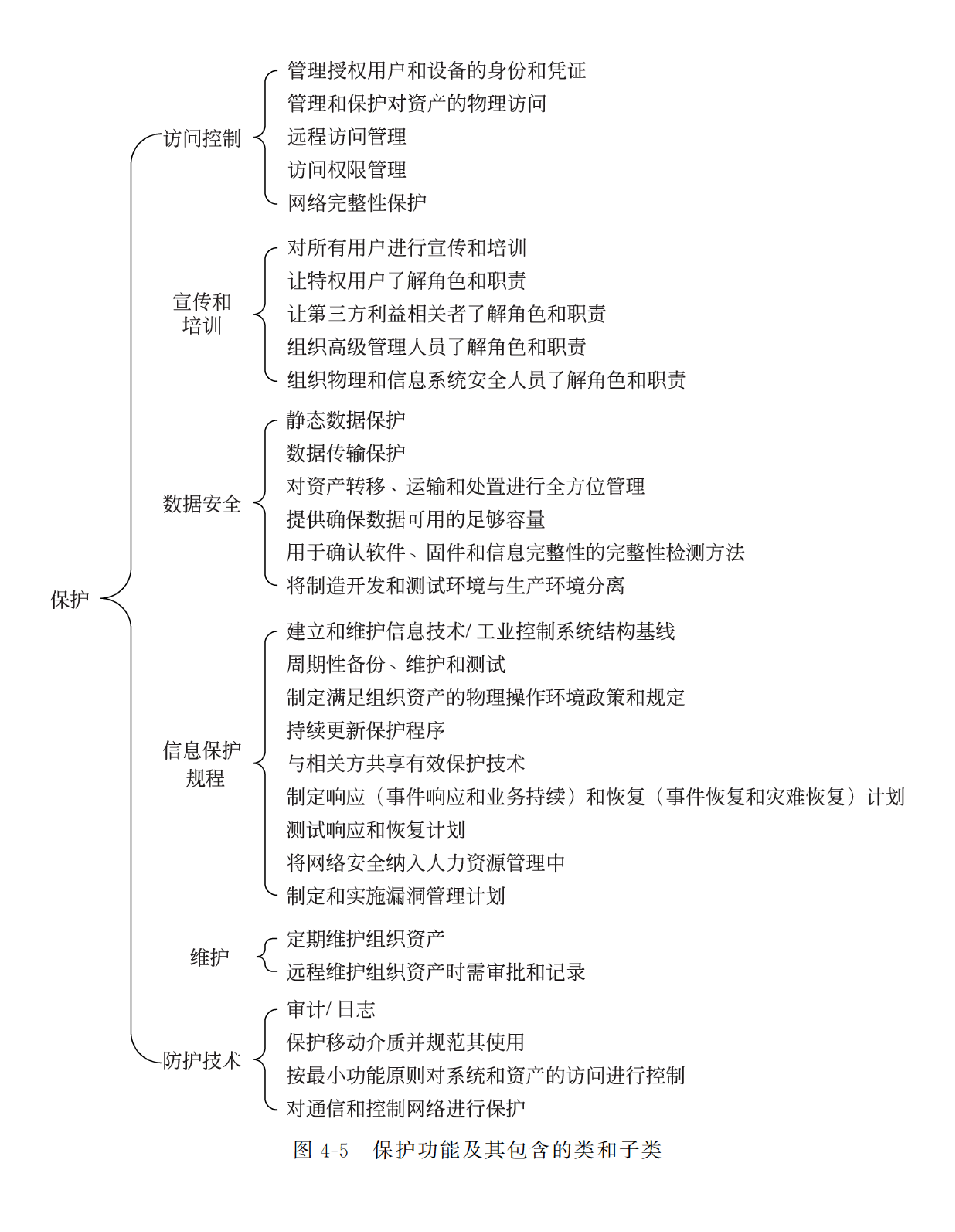


图 4-5　保护功能及其包含的类和子类

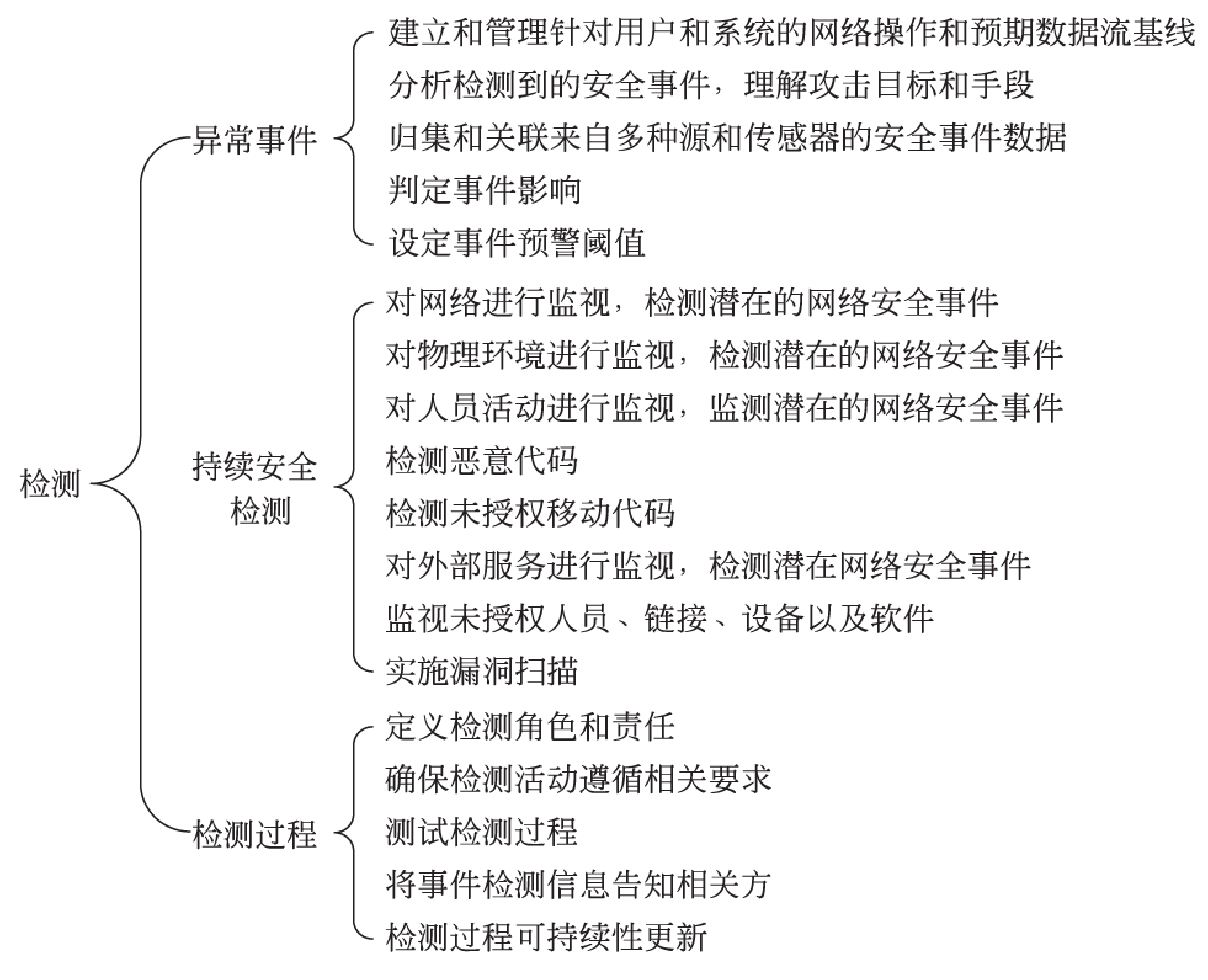


图 4-6　检测功能及其包含的类和子类

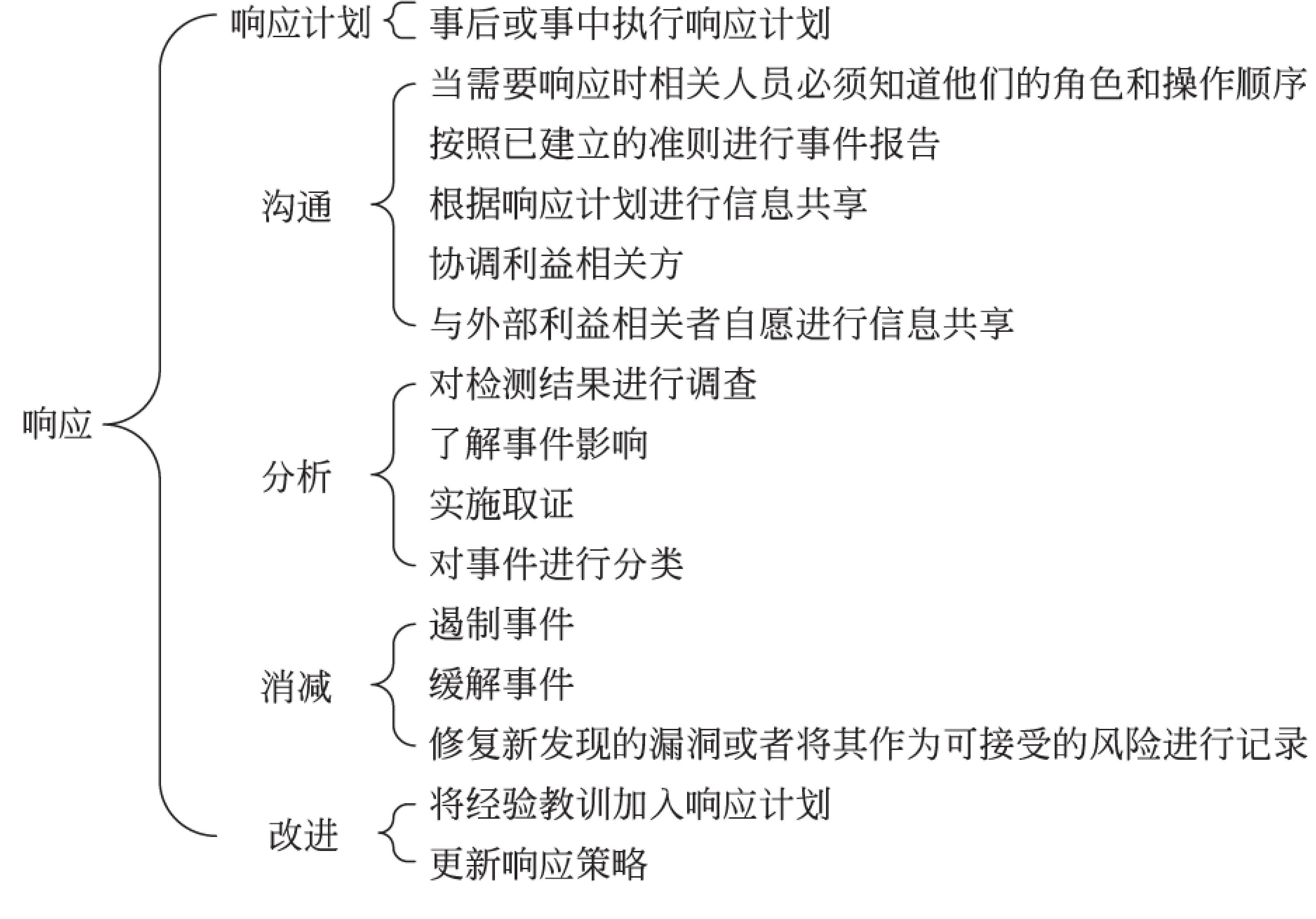


图 4-7　响应功能及其包含的类和子类

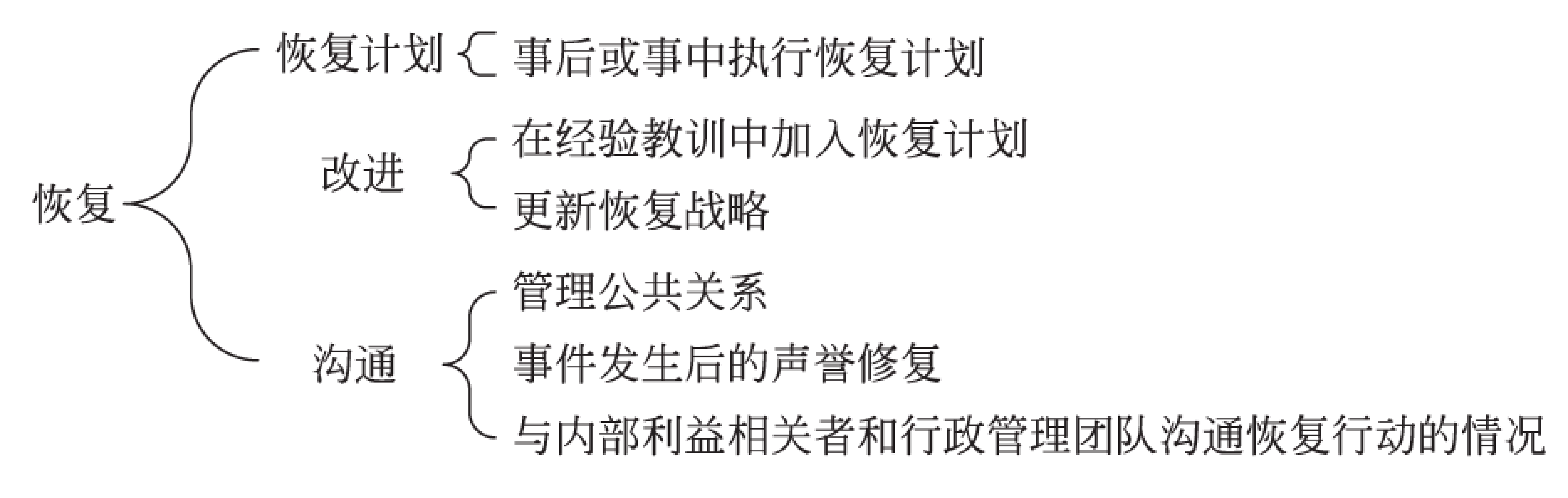


图 4-8　恢复功能及其包含的类和子类

(4)“参考性文献”包括一系列与“子类”提出的安全要求相对应的,适用于关键基础设施的已有安全标准、指南和实践。“功能”“类”“子类”均只给出了逐步细化的安全目标,但并没有对如何实现安全目标提出具体要求。这些具体要求则在“参考性文献”所列出的标准、指南和实践的具体条款中体现。也就是说,框架没有提出任何新的安全要求,只是明确了若干安全目标,并将安全目标的实现措施指向了已有标准、指南和实践的具体条款。之所以称之为“参考性文献”,旨在说明这些引用的标准、指南和实践并不是强制性的,且可供参考的标准、指南和时间也并不仅限于此。框架中列出的“参考性文献”主要有:

(1) 信息和相关技术控制目标(Control Objectives for Information and Related Technology,COBIT)。

(2) 网络安全理事会(Council on CyberSecurity,CCS)前 20 位关键安全控制。

(3) ANSI/ISA-62443-2-1-2009《工业自动化和控制系统安全:建立工业自动化和控制系统安全计划》。

(4) ANSI/ISA-62443-3-3-2013《工业自动化和控制系统安全:系统安全要求和安全等级》。

(5) ISO/IEC 27001《信息技术　安全技术　信息安全管理体系要求》。

(6) NIST SP 800-53 Rev. 4《联邦信息系统和组织的安全和隐私控制》。

4.2.3　框架实现层级

框架实现层级为不同单位分析网络安全风险,以及如何结合自己的实际情况来实现框架提供了具体的规定说明。根据单位本身对于安全风险的认知和应对水平(是否制定了风险管理方法和综合风险管理计划,是否参与外部单位的安全风险评估活动),总共的框架实现层级包括 4 个层次,即部分实现、风险告知、可重复、自适应。当组织者制定自己的框架实现层级时,应考虑其当前所处的安全风险环境、风险管理实际状况、信息安全防护目标、法律法规要求及相关的约束条件等。

1. 框架实现层级之“部分实现”

（1）风险管理方法。风险管理以临时和反应式的方式进行。网络安全应对措施的优先顺序不以单位的风险目标或业务需求为导向。

（2）综合风险管理计划。单位对网络安全风险知之甚少，且未建立内部网络安全风险管理措施。网络安全风险管理工作没有正式规程，或仅从外部获得安全事件信息。单位内部未制定网络安全信息共享流程。

（3）参与外部单位的安全风险评估活动。单位没有参加其他单位的安全风险评估活动，没有形成与其他单位协调或合作的机制。

2. 框架实现层级之“风险告知”

（1）风险管理方法。单位制定的网络风险管理具体实践方法已经通过了单位管理部门的批准，但没有制定单位内部的风险管理通用策略。网络安全应对措施的优先顺序是以单位的风险目标或业务需求为导向的。

（2）综合风险管理计划。单位已经意识到了网络安全风险问题，但未形成内部网络风险管理措施。单位已经制定并批准实施了综合风险管理计划，单位员工拥有充足的网络资源来履行网络安全职责。单位制定了网络安全信息共享流程，员工可在单位内部开展日常安全信息交流与共享工作。

（3）参与外部单位的安全风险评估活动。单位已经认识到了与其他单位开展安全风险协同评估活动的重要性，并明确了自己在协同工作中所扮演的角色，但是仍无法有效履行其职责。

3. 框架实现层级之“可重复”

（1）风险管理方法。单位制定的网络风险管理具体实践方法已经被正式公布了，并且进一步制定了单位内部的风险管理通用策略。单位实施的网络安全实践要基于具体应用的业务需求、安全威胁和技术发展趋势等因素来定期进行更新改进。

（2）综合风险管理计划。单位制定了网络风险管理措施，明确了风险告知政策和流程。这些政策和流程在实施之后，经受实际安全事件的检验，评审其正确性和有效性。此外，单位已经制定了一套能够有效应对不断变化的安全风险的通用方法。单位员工已经掌握了相关网络安全专业知识和技能，可以胜任他们的安全角色和职责。

（3）参与外部单位的安全风险评估活动。单位已经清晰地理解自己在与其

他单位开展安全风险协同评估活动中所扮演的角色和职责。而且单位也清楚地认识了在单位内部开展安全风险评估过程中，对其他单位的安全风险评估信息的依赖性。

4. 框架实现层级之“自适应”

(1) 风险管理方法。基于对历史经验教训的总结和未来网络安全威胁发展趋势的预测，单位能够及时调整其网络安全管理方法。并且，通过不断融入先进的网络安全技术和实践，单位可以不断地主动调整其网络安全防护措施，以此来及时应对错综复杂的网络安全威胁。

(2) 综合风险管理计划。单位制定了网络风险管理措施，明确了风险告知政策和流程。单位可以利用这些管理措施、风险告知政策和流程，有效应对潜在的网络安全事件。网络风险管理已经成为企业文化的一部分。并且，单位还会通过分析之前的安全事件，与其他单位共享安全事件分析结果，不断监测单位的网络系统安全态势等手段来不断改进综合风险管理计划。

(3) 参与外部单位的安全风险评估活动。单位与合作伙伴单位一起积极主动地开展安全事件信息共享合作，确保在网络安全事件发生前，及时、准确地传递安全威胁信息。

4.2.4 框架配置文件

框架配置文件代表了一个单位在基于信息安全需求所选定的框架实现层级和“功能”、“类”、“子类”以及“参考性文献”的具体内容。在一个实际的框架实现过程中，框架配置文件可以被看做是一种针对信息安全防护标准、指导意见和安全实践等文件的对标文件。单位要制定一个框架配置文件，那么它可以先查看框架核心中的所有类别和子类别，基于自己所需要的信息安全需求，对安全防护措施进行优先级排序，或按照自己的需求来进行定制选择。此外，框架配置文件也可以被单位用来作为进行自我评估或者与其他单位进行信息沟通的工具。

图 4-9 描述了在组织内部的主管(Executive)人员、业务流程(Business/Process)人员、实施操作(Implementation/Operations)人员之间所采用的通用风险管理信息与决策流程模型。主管人员给业务流程人员设定任务优先级、可用资源以及对风险的承受能力，业务流程人员根据这些信息和风险管理方法，与实施操作人员沟通安全需求和业务需求并创建配置文件。实施操作人员跟业务流程人员沟通配置文件的具体实施结果信息。业务流程人员根据这些信息进行安全评估，并将其评估结果反馈给主管人员。

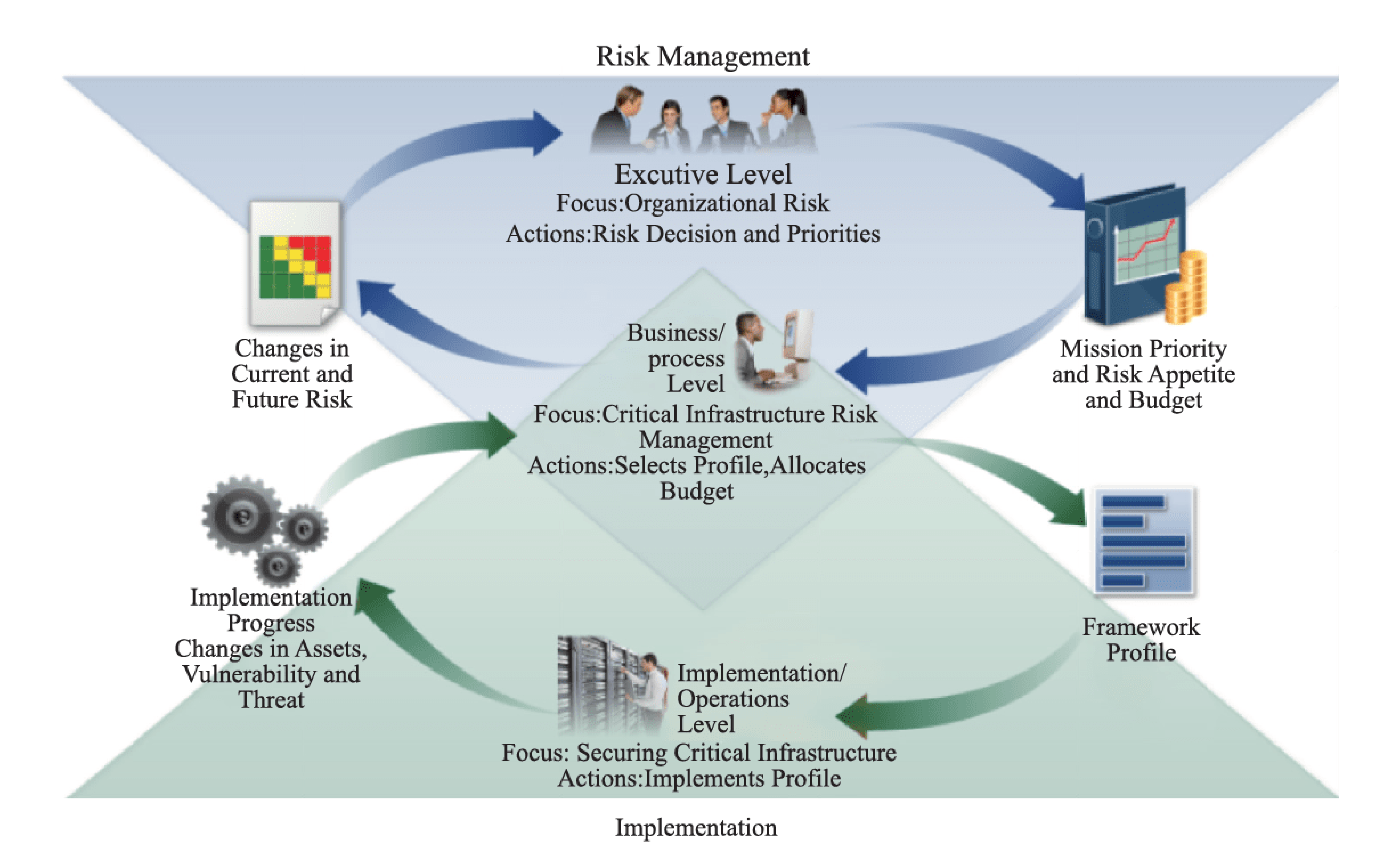


图 4-9 风险管理的信息与决策流程模型(来源：文献[2] Figure 2)

4.2.5 框架使用方法

单位可以将提高关键基础设施网络安全的框架作为识别、评估和管理网络安全风险的核心体系。本框架并不是用来取代单位现有的网络安全风险管理方法的，而是在现有方法基础上来分析不足和差距，以此来制定发展和改进的技术路线。至于本框架的使用方法，具体包括以下几点。

1. 对本单位的网络安全进行基本的安全审查

在本规范建立的框架中，框架核心可以被单位用作开展自我安全审查工作的依据。单位通过建立一个当前的框架配置文件，就可以针对框架核心五个“功能”(识别、保护、检测、响应和恢复)中的“类”和“子类”进行自检，梳理本单位的安全现状。如果单位发现目前的安全风险管理方法已经能够达到预定的安全目标，那么就可以利用现有方法来管理已知的安全风险。反之，单位可以通过自我安全审查发现不足，以此来制定一个安全改进计划。但是，如果单位发现目前在某个“功能”(或“类”“子类”)的安全风险投入已经远远超出安全目标产出的话，那么单位就可以将这部分的资源分配给其他的方面。

2. 建立或改进一个网络安全项目

单位可以参考以下 7 个步骤来建立或改进一个网络安全项目。单位应该不断执行这些步骤，进而持续地提升自身网络安全等级。

步骤 1：单位设定安全范畴并制定安全需求的优先级。

单位可以根据对应的网络安全实践来制定战略决策，决定企业系统和资产的保护范畴。框架可以在经过调整之后，在单位内部用来支持不同的企业业务种类和流程。这些业务种类和流程可能会有不同的安全需求和相应的安全风险容忍能力。

步骤 2：单位确定提升安全等级方向。

一旦网络安全项目的安全范畴确定了之后，单位就可以清点其内部系统和资产，明确安全要求。单位接下来就可以识别系统和资产的脆弱性和安全威胁。

步骤 3：单位创建一个目前的框架配置文件。

单位建立一个能够包含“功能”、“类”和“子类”的框架配置文件，以此来表征其目前的安全等级。

步骤 4：单位开展安全风险评估工作。

单位可以根据其安全风险管理方法和之前的安全风险评估工作情况来开展目前的安全风险评估工作。单位通过分析系统运行环境，来识别未来网络安全事件发生的概率，并预测其安全危害。此外，单位还应该考虑新兴的网络安全风险、威胁和脆弱性对自身系统的潜在安全影响。

步骤 5：单位建立一个目标框架配置文件。

单位根据预期达到的安全目标来建立一个目标框架配置文件。该配置文件用来描述单位在“功能”、“类”和“子类”等方面要达到的安全目标。单位也可以根据自己的实际情况量身定制符合自身需求的额外的“功能”、“类”或“子类”。此外，单位在制定目标框架配置文件的时候，还需要考虑客户、商业合作伙伴的安全需求。

步骤 6：单位分析并确定目标框架配置文件与目前的框架配置文件之间的差距。

单位通过对比目前的框架配置文件和目标框架配置文件，分析并确定二者的安全差距，制定行动计划。接下来，单位需要通过权衡分析安全风险和安全改进所带来的代价，对缩短安全差距所需要采取的行动制定优先级。

步骤 7：实现安全行动计划

单位依据制定的目标框架配置文件，参照其中的参考性文献（如安全标准、

指导建议和安全实践)来实现安全行动计划,直至实现目标框架配置文件中所述的所有“功能”、“类”或“子类”。

3. 单位与利益相关者沟通网络安全需求

本规范建立的框架配置文件,可以作为不同利益相关者之间相互沟通交流安全需求的一种通信语言。这有利于提高不同利益相关者之间的沟通效率。单位可以用其目标框架配置文件来表达自己对其他单位服务提供商的安全要求(如云服务用户可以对云服务提供商描述自己对云数据安全的要求)。一个关键基础设施的拥有者或运营者,已经意识到了自身对一个外部合作单位系统的依赖性,此时这个拥有者或运营者就可以使用一个框架配置文件来向合作单位说明自身对“功能”、“类”或“子类”的要求。

4. 引入新的参考性文献

本规范建立的框架鼓励单位通过引入新的参考性文献来提高框架的普适性。

5. 保障隐私和公民自由

本框架需要采取一定的方法来保障单位及个人的隐私和自由权。

4.2.6 规范小结

NIST 通过将所有这些资料集成到一个统一的知识库里,为组织评估自身安全准备水平和自我定位提供了一套通行的术语和方法论。本规范为实现网络安全实践提供了一个通用框架,但并非是预防网络攻击和数据泄露的万能解决方案。我们要清楚地意识到,指导方针和条例规程本质上是静态的,因而不能检测和减轻不断变化的安全威胁。同时,安全防护标准也远远跟不上网络攻击的脚步。合理的安全措施和最佳实践只是解决方案中的一部分。要想有效预防网络攻击,除了技术上的手段,还得结合必要的大数据分析方法,从大量的安全反馈信息中进行快速及时的分析和响应。从这个意义上说,本规范确实是一块重要的基石,但只是通往实现抵御网络安全风险的第一步。

4.3 工业控制系统安全指南

《工业控制系统安全指南》[1]文档用于指导建立安全工业控制系统(SCADA、DCS、PLC),本文给出了工业控制系统(ICS)简介,综述了典型的 ICS

系统架构和拓扑，指出了已知的安全威胁和系统脆弱性，并针对这些安全风险提供了安全对策和建议。具体指出了以下安全目标：限制对 ICS 网络及其网络活动的逻辑访问；在开发过程中保证 ICS 组件安全；防止对数据的非授权访问；能检测出安全事件，在发生攻击、故障等不利情况下，能够保证 ICS 功能正常运转；能够在发生安全事件后进行及时有效的恢复。

SP 800-82 有逻辑地给出了 ICS 安全保护的建议和指导，若能有效地满足这样的需求，ICS 系统就可达到更安全的(secure)，即系统处在一种特定状态，可有效地抵御所面临的不可接受的风险。

该指南为保障工业控制系统 ICS 提供指南，包括数据采集与监控系统(SCADA)、分布式控制系统(DCS)和其他完成控制功能的系统。它概述了 ICS 和典型的系统拓扑结构，指出了这些系统的典型威胁和脆弱点所在，为消减相关风险提供了建议性的安全对策。同时，根据 ICS 的潜在风险和影响水平的不同，指出了保障 ICS 安全的不同方法和技术手段。该指南适用于电力、水利、石化、交通、化工、制药等行业的 ICS 系统。

典型的工业控制系统包括数据采集和监视系统(SCADA)、分布式控制系统(DCS)以及可编程逻辑控制器(PLC)。

如图 4-10 所示，ICS 操作关键组件包括控制回路、人机界面(HMI)、远程诊断和维护工具。

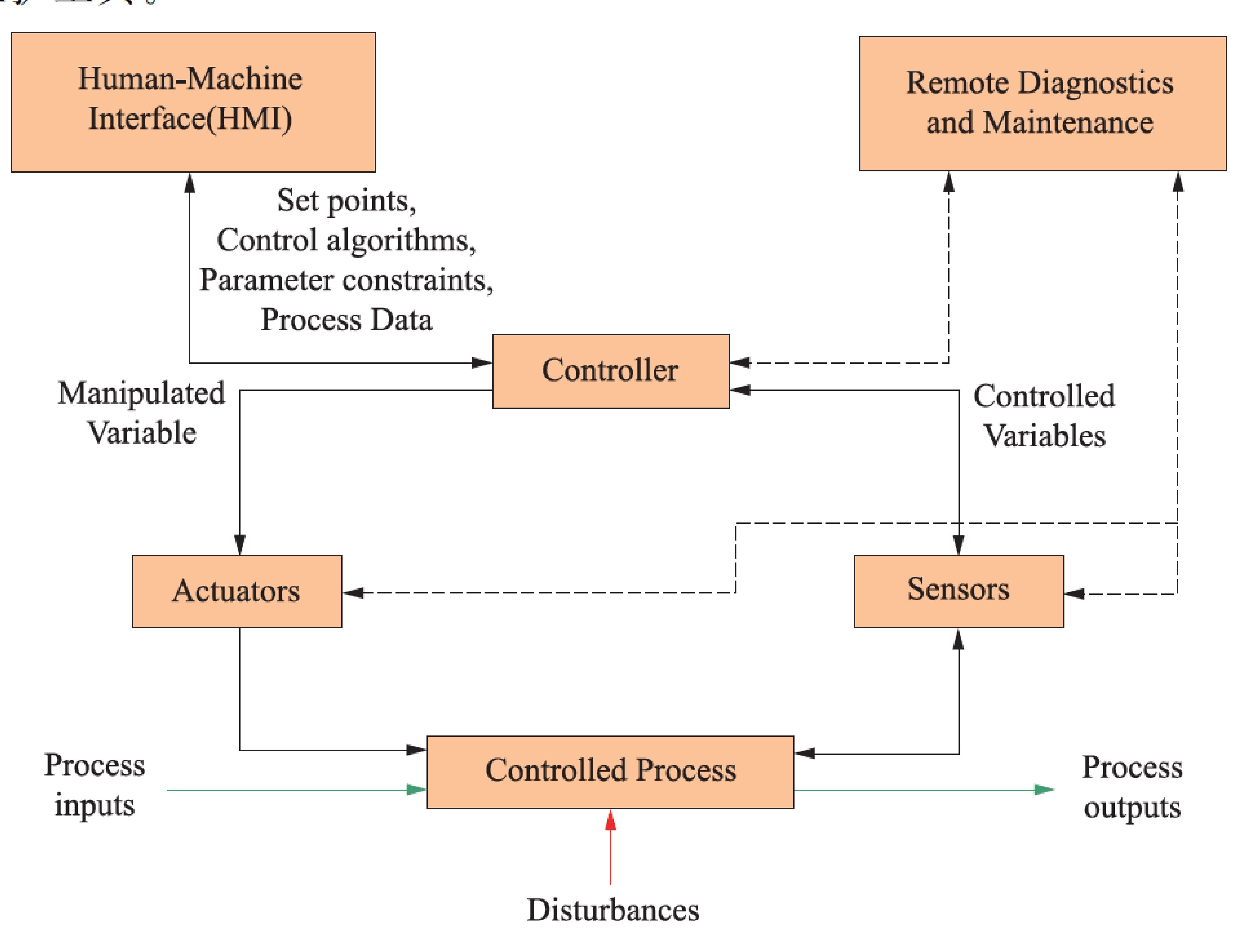


图 4-10　ICS 操作(来源：文献[1] Figure 2-1)

根据功能划分,主要的 ICS 元件可以分为控制元件和网络组件。控制元件包括控制器、SCADA 服务器或主终端单元(MTU)、远程终端装置(RTU)、可编程逻辑控制器(PLC)、智能电子设备(IED)、人机界面(HMI)、历史数据库、输入输出(I/O)服务器。网络组件有总线网络、控制网络、通信路由器、防火墙、调制解调器、远程接入点。

SCADA 系统是用来控制地理上分散的资产的高度分布式系统,往往分散数千平方公里,其中集中的数据采集和控制是系统运行的关键。这些系统被用于配水系统和污水收集系统、石油和天然气管道、电力设施的输电和配电系统以及铁路和其他公共交通系统。系统的总体结构如图 4-11 所示。

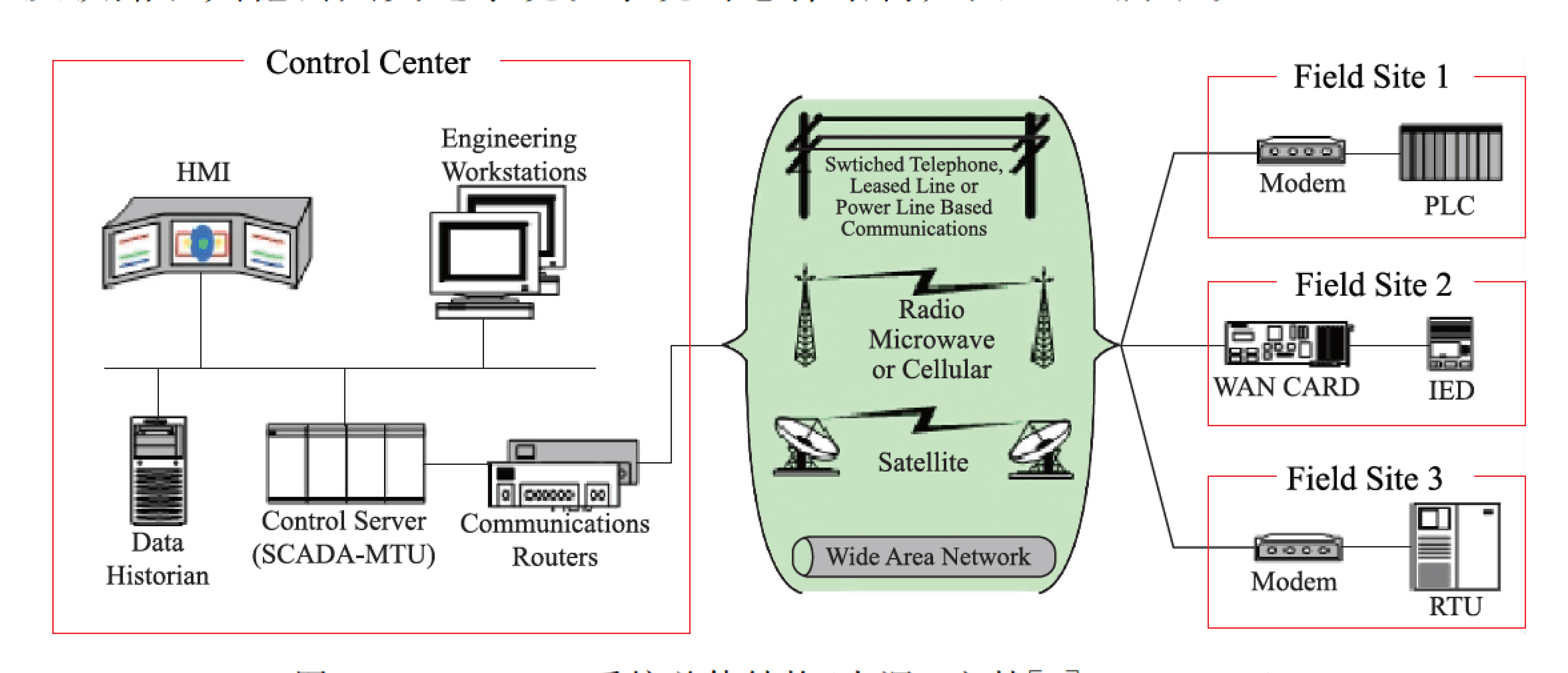


图 4-11　SCADA 系统总体结构(来源:文献[1] Figure 2-2)

分布式控制系统(DCS)用于控制在同一地理位置的生产系统,被用来控制工业生产过程,如炼油厂、水和污水处理、发电设备、化学品制造工厂和医药加工设施等行业。可编程逻辑控制器(PLC)可用在 SCADA 和 DCS 系统中,作为整个分级系统的控制部件,通过反馈控制,提供对过程的本地管理。图 4-12 给出了一个 DCS 系统实例。

4.3.1　ICS 特性

起初,ICS 与 IT 系统并无相似之处。随着 ICS 采用广泛使用的、低成本的互联网协议(IP)设备取代专有的解决方案,以促进企业连接和远程访问能力,并正在使用行业标准的计算机、操作系统(OS)和网络协议进行设计和实施,它们已经开始类似于 IT 系统了。但是 ICS 有许多区别于传统 IT 系统的特点,包括不同的风险和优先级别。其中包括对人类健康和生命安全的重大风险,对环境的严重破坏,以及金融问题如生产损失和对国家经济的负面影响。表 4-1 总结了一些 IT 系统和 ICS 之间的典型差异。

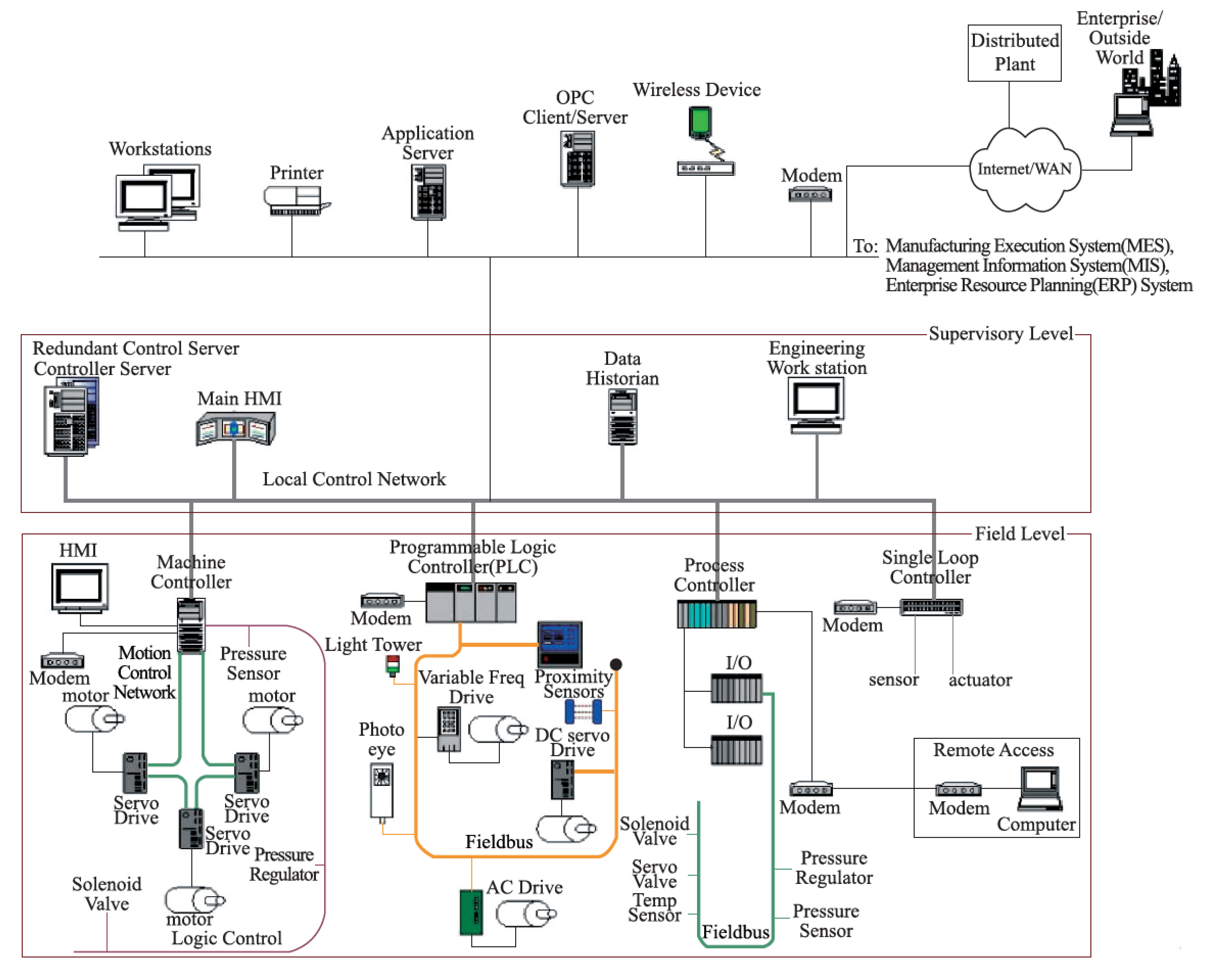


图 4-12　DCS 系统实例(来源:文献[1] Figure 2-7)

表 4-1　IT 系统和 ICS 的差异总结

分类	信息技术系统	工业控制系统
性能需求	• 非实时 • 响应必须是一致的 • 要求高吞吐量 • 高延迟和抖动是可以接受的	• 实时 • 响应是时间紧迫的 • 适度的吞吐量是可以接受的 • 高延迟和(或)抖动是不能接受的
可用性需求	• 重新启动之类的响应是可以接受的 • 可用性的缺陷往往可以容忍的,当然要取决于系统的操作要求	• 重新启动之类的响应可能是不能接受的,因为过程的可用性要求 • 可用性要求可能需要冗余系统 • 中断必须有计划和提前预订时间(天/周) • 高可用性需要详尽的部署前测试

续表

分类	信息技术系统	工业控制系统
管理需求	• 数据保密性和完整性是最重要的 • 容错是不太重要的-临时停机不是一个主要的风险 • 主要的风险影响是业务操作的延迟	• 人身安全是最重要的，其次是过程保护 • 容错是必不可少的，即使是瞬间的停机也可能无法接受 • 主要的风险影响是不合规，环境影响，生命、设备或生产损失
体系架构安全焦点	• 首要焦点是保护 IT 资产，以及在这些资产上存储和相互之间传输的信息 • 中央服务器可能需要更多的保护	• 首要目标是保护边缘客户端（例如现场设备、过程控制器） • 中央服务器的保护也很重要
未预期的后果	安全解决方案围绕典型的 IT 系统进行设计	安全工具必须先测试（例如，在参考 ICS 上的离线），以确保它们不会影响 ICS 的正常运作
时间紧迫的交互	• 紧急交互不太重要 • 可以根据必要的安全程度实施严格限制的访问控制	• 对人和其他紧急交互的响应是关键 • 应严格控制对 ICS 的访问，但不应妨碍或干扰人机交互
系统操作	• 系统被设计为使用典型的操作系统 • 采用自动部署工具使得升级非常简单	• 与众不同且可能是专有的操作系统，往往没有内置的安全功能 • 软件变更必须小心进行，通常是由软件供应商操作，因其专用的控制算法，以及可能要修改相关的硬件和软件
资源限制	系统被指定足够的资源来支持附加的第三方应用程序如安全解决方案	系统被设计为支持预期的工业过程，可能没有足够的内存和计算资源以支持附加的安全功能

续表

分类	信息技术系统	工业控制系统
通信	• 标准通信协议 • 主要是有线网络，稍带一些本地化的无线功能的 • 典型的 IT 网络实践	• 许多专有的和标准的通信协议 • 使用多种类型的传播媒介，包括专用的有线和无线(无线电和卫星) • 网络是复杂的，有时需要控制工程师的专业知识
变更管理	在具有良好的安全策略和程序时，软件变更是及时应用的，往往是自动化的程序	软件变更必须进行彻底的测试，以递增方式部署到整个系统，以确保控制系统的完整性。ICS 的中断往往必须有计划，并提前预订时间(天/周)。ICS 可以使用不再被厂商支持的操作系统
管理支持	允许多元化的支持模式	服务支持通常是依赖单一供应商
组件生命周期	3～5 年的生存期	15～20 年的生存期
组件访问	组件通常在本地，可方便地访问	组件可以是隔离的、远程的，需要大量的物力才能获得对其的访问

工业控制系统面临的威胁可以来自多种来源，包括对抗性来源如敌对政府、恐怖组织、工业间谍、心怀不满的员工、恶意入侵者，自然来源如系统的复杂性、人为错误和意外事故、设备故障和自然灾害。

如图 4-13 所示，工业控制系统潜在的脆弱性被划分为策略与程序类、平台类和网络类脆弱性，在工业控制系统中常出现的一些脆弱性都可归集到这几类中。

随着 ICS 系统越来越多地采用标准化的协议和技术，许多安全漏洞已知，连接到其他网络控制系统，不安全和非法的网络连接以及系统相关技术信息的广泛普及导致 ICS 控制系统风险的日益增加。

4.3.2 ICS 系统安全程序开发与部署

ICS 和 IT 系统之间存在较大的差异，这将影响 ICS 系统采用何种安全控制措施。ICS 系统拥有者或运营者应制定和部署 ICS 安全策略与程序，这些安全策略与程序必须符合 ICS 在技术和环境方面的具体安全需求。拥有者或运营者应定期审查和更新他们的 ICS 安全计划和方案，以适应新技术、业务、标准和法规的要求。如图 4-14 所示，开发与部署 ICS 安全项目包括六个步骤：建立一个 ICS 安全防护商业案例，创建和培养一个多功能安全人才团队，制定安全章程和安全保护范畴，制定 ICS 安全策略和安全措施实施流程，开发实现 ICS 安全风险

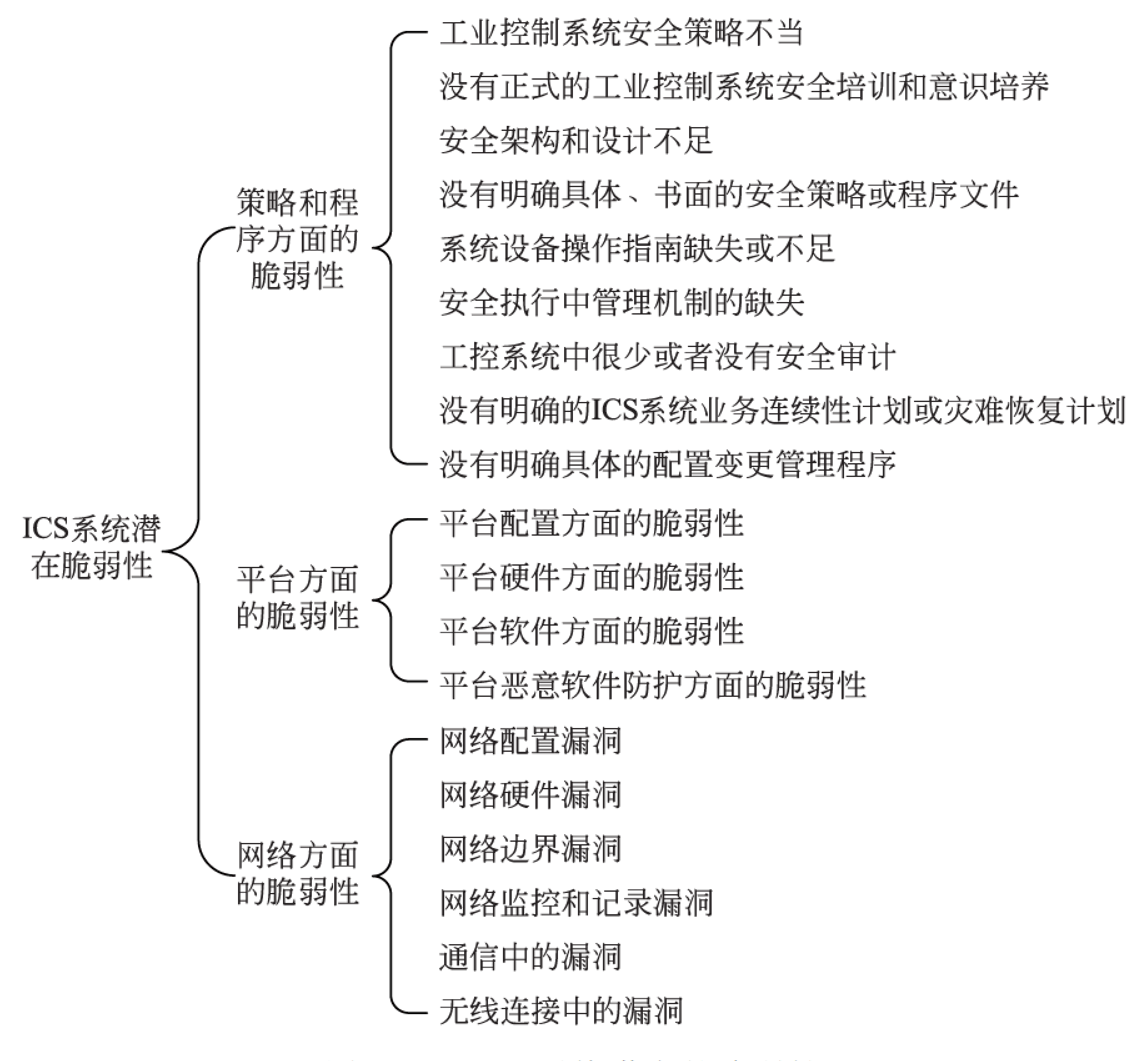


图 4-13　ICS 系统潜在的脆弱性

管理框架，培训 ICS 员工的安全意识和安全技能。

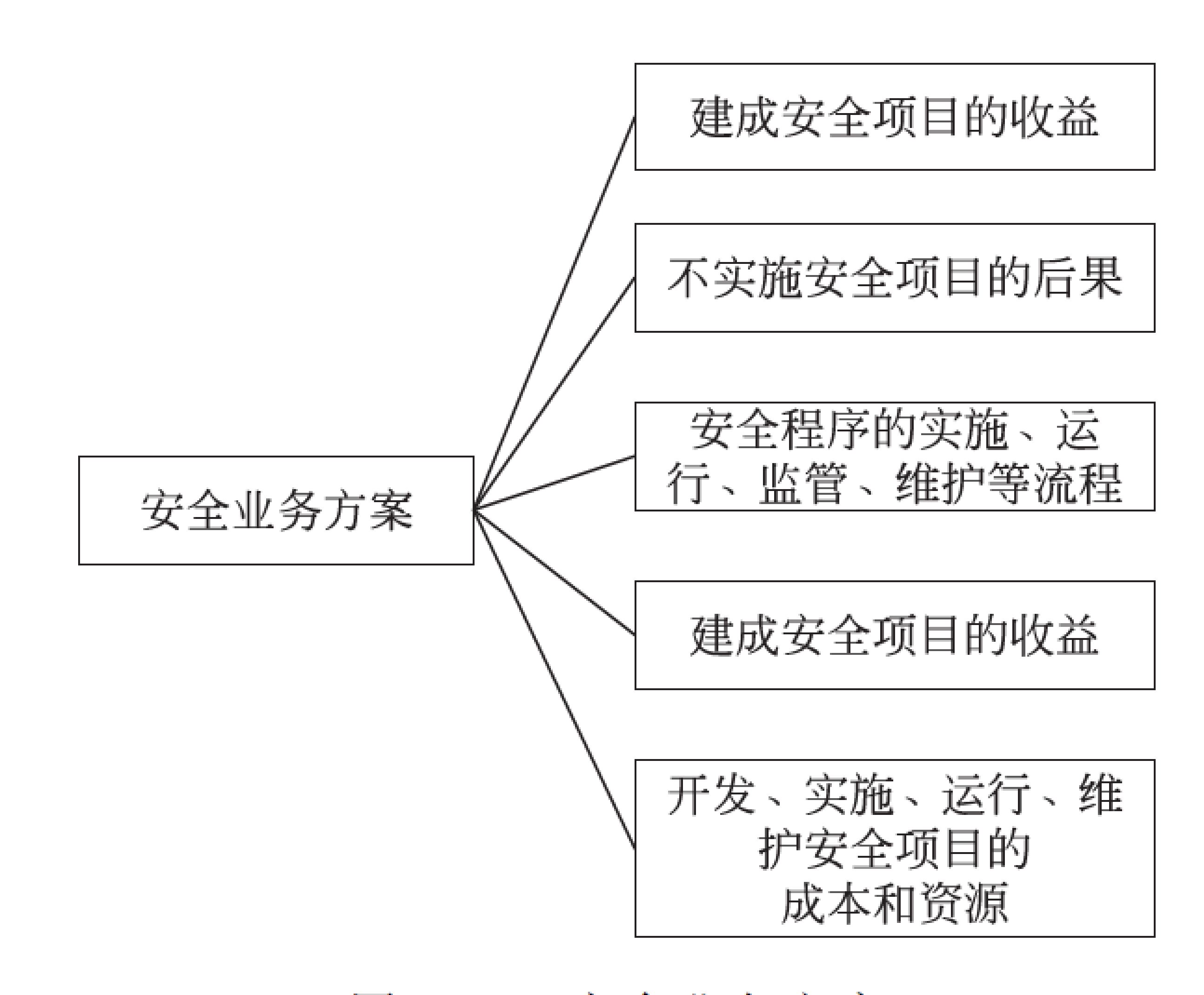


图 4-14　安全业务方案

1. 建立一个 ICS 安全防护商业案例

开发与部署 ICS 安全项目的第一步就是要针对 ICS 系统提供商、拥有者或运营

者等单位的安全需求，定制一个 ICS 安全防护商业案例。该案例应该能够涵盖并有效解决这些单位领导管理者们所关心的安全问题。案例应该包括以下四方面内容：

（1）如果单位建立一个 ICS 系统安全防护项目，能给单位带来多大的收益；

（2）如果单位没有实施 ICS 系统安全项目的话，那么单位将有可能遭受多大的经济损失和破坏；

（3）案例应给出一个关于安全防护项目实施、运作、监测、审查、维护和改进的概略介绍，让领导管理者们能够对整个项目有个全面的了解；

（4）案例还应该给出一个关于开展安全防护项目所需付出的经济开销和网络（或系统）资源开销等。

2. 创建和培养一个多功能安全人才团队

在开发和部署 ICS 系统安全防护项目过程中，创建一个多功能安全人才队伍对于项目的成功实施来说是至关重要的。这个团队的人员应该包括 IT 员工、控制系统工程师、控制系统操控者、信息安全专家及企业风险管理部门员工。这些多功能安全人才拥有网络架构、安全控制过程和实践、安全基础设施设计和运行等不同领域的专业技术知识，一起协同合作评估 ICS 系统的安全威胁，并商讨消除安全威胁的办法。

虽然工业控制工程师在 ICS 安全防护方面扮演了举足轻重的角色，但是如果没有 IT 部门和管理部门的大力支持，他们也无法完成 ICS 安全防护工作。IT 人员拥有丰富的信息安全经验，这些经验可以指导工业控制工程师开展 ICS 安全防护工作。尽管 IT 人员和工业控制工程师的技术背景相差甚远，但是二者的结合对于开展 ICS 安全防护工作来说却是必需的。

3. 制定安全章程和安全保护范畴

信息安全管理者应该在控制系统拥有者、业务流程管理者和用户的信息安全角色和职责等方面，制定安全章程和安全保护范畴。关于信息安全项目目标、商业影响、涉及的计算机系统和网络、项目预算和资源开销以及责任分工等因素，信息安全管理者应该做出明确的章程并形成书面文件。至于安全保护范畴，信息安全管理者则应该规定开展安全培训和审计、制定安全法律、法规等工作所涉及的范围。

4. 制定 ICS 安全策略和安全措施实施流程

安全策略和安全措施实施流程是安全防护项目成功开展的基础。ICS 安全

策略和安全措施实施流程应该尽可能地整合现有工业控制操作和管理策略和流程。当信息安全管理者确定了信息安全风险分析方法之后，就应该对照分析现有安全策略是否能够满足安全需求。如果需要的话，信息安全管理者也可以在现有安全策略基础上来改进或者重新制定新的策略。

5. 开发实现 ICS 安全风险管理框架

NIST SP 800-39《从组织、任务和信息系统角度管理信息安全风险》[8] 为开展安全风险管理项目提供了理论基础。该标准指出，与其他领域业务流程类似，在工业控制系统中，安全人员应该利用他们的专业知识来开展 ICS 安全风险管理工作，并与企业管理层沟通，以此来为整个企业提供有效的安全风险管理保障。NIST SP 800-37《联邦政府信息系统安全风险管理框架实施指南》[9] 为联邦政府实施信息系统安全风险管理框架，给出了具体的指导意见。此外，ISA-62443-2-1《工业自动化和控制系统安全：建立一个工业自动化和控制系统安全项目》标准[10]，以工业自动化和控制系统视角，介绍了应该如何部署网络安全管理系统。信息安全管理者应该参照上述现有标准，通过确定 ICS 系统与网络资产，确定不同 ICS 安全风险优先级，实施安全风险评估，实施安全风险消除措施等步骤来开发实现 ICS 安全风险管理框架。详细的 ICS 安全项目开发流程可以参见图 4-15。

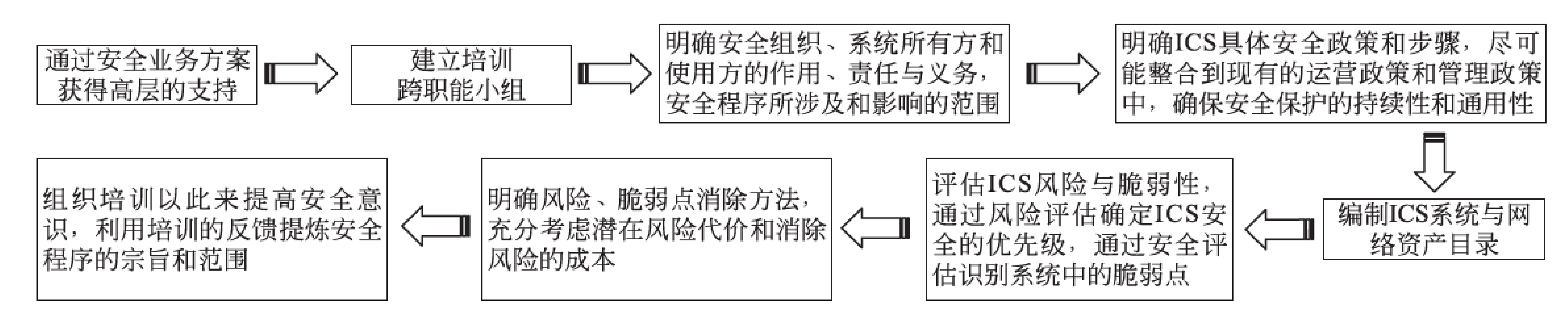


图 4-15　综合安全程序的开发

4.3.3 深度防御架构

在系统安全建设的环节中，除了安全程序开发，另一个关键环节是处理好 ICS 网络与其他应用网络的连接问题，以及网络体系结构问题。当设计部署含有 ICS 系统的网络架构时，通常的建议是将 ICS 网络和企业网络进行分离，这种情况下，企业网的安全和性能问题不会影响 ICS 网络。当必须需要连接时，强烈建议仅进行最小连接并通过防火墙和 DMZ 区进行连接。DMZ 区是直接连接在防火墙上的独立网络分区。需要访问企业网络的 ICS 系统数据服务器一般放在 DMZ 区。如图 4-16 所示，关于深度防御体系结构，本指南给出了以下建议：

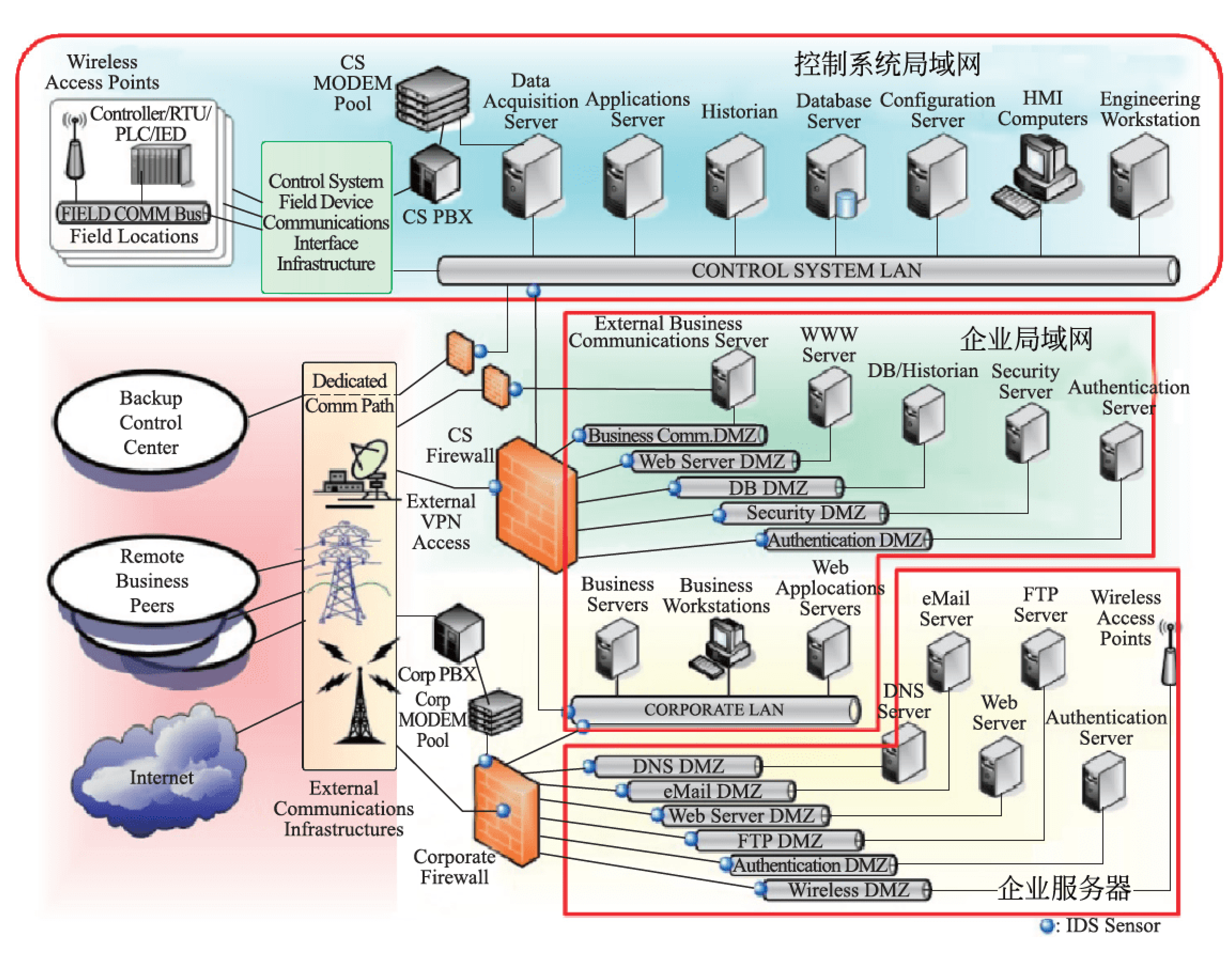


图 4-16　CSSP 建议的深度防御架构(来源：文献[1] Figure 5-5)

1. 网络划分和隔离

传统意义上，网络隔离和分区应用在区域之间的网关上。ICS 通常由多种定义的区域，例如，控制系统局域网、企业局域网等。网络分区常用的方法有逻辑网络分区(划分 VLAN、使用加密 VPN、使用单向网关)、物理网络分区和网络流量过滤等。

2. 边界保护

边界保护包括网关、路由器、防火墙、保护装置、基于网络的恶意代码分析和虚拟化系统、入侵检测系统、加密通道、监管接口、邮件网关和单相网关等。常用的技术主要有白名单技术、服务器代理、数据深度检测等。

3. 控制网络的逻辑隔离

比较可行的一种逻辑隔离方式是在 ICS 网络和企业网络之间实施 DMZ 区，只有指定的数据才能在企业网和 DMZ 区以及 ICS 网络和 DMZ 区之间进行通信，使企业网络和 ICS 网络不能直接进行数据交换。

4. 网络隔离

常见的网络隔离的形式有使用双宿主计算机/双网卡、企业网络和控制网络之间使用防火墙、防火墙和路由器、防火墙和 DMZ 区、双冗余防火墙几种方式之一。更深一步的网络隔离策略是使用深度防御架构，相关策略包括使用防火墙、创建 DMZ 区、具有有效策略的入侵检测能力、培训计划以及事件响应机制。图 4-16 为 DHS 控制系统安全项目推荐的一种深度纵深防御架构。

4.3.4 ICS 安全控制

安全控制是信息系统为了保护其信息的保密性、完整性和有效性而制定的一套管理、操作和技术控制方法。本“指南”主要是将 NIST SP 800-53[11] 中“联邦信息系统与组织安全控制方法”部分提出的管理、运营和技术方面的控制措施运用在 ICS 中。NISP SP 800-53 是针对联邦政府信息系统，为信息系统选择和指定安全控制方法而提出的准则。如图 4-17 所示，安全控制分为三个等级：管

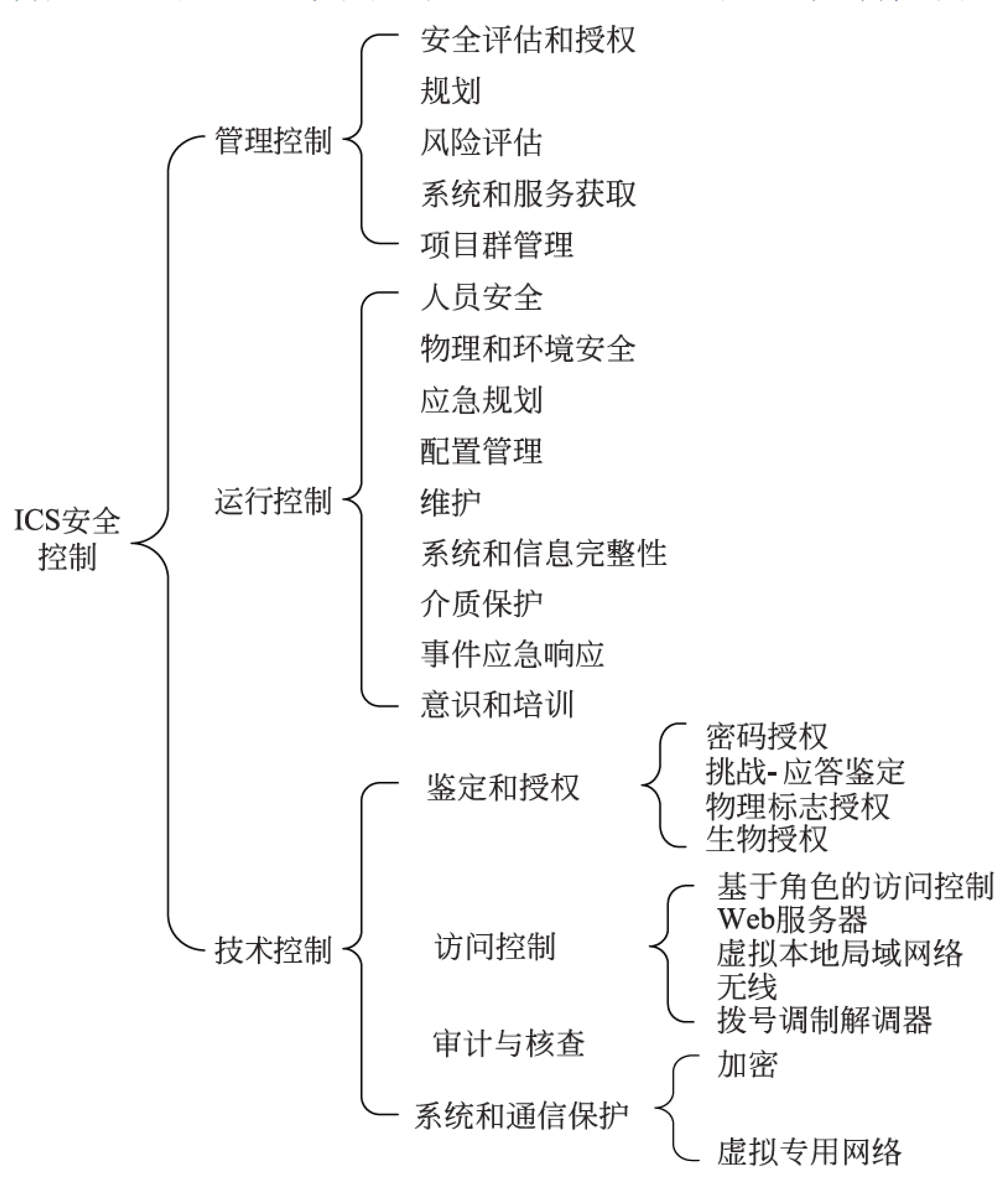


图 4-17　ICS 安全控制

理控制、运行控制和技术控制。

4.4　工业控制系统网络安全性能测试床

NIST 开展的工业控制系统网络安全性能测试床[12]的目的是，在国家和国际标准提供的最佳实践和需求的网络安全保护的基础上衡量 ICS 的性能。测试床的目标就是尽可能地仿真实际的 ICS，包括慢过程系统和快过程系统。测试床还仿真各种工业协议，包括 IP 路由协议和非 IP 路由协议。路由协议包括基于 IP 的协议（如 TCP 和 UDP）以及工业应用层协议（如 EtherNet/IP、OPC、Modbus/TCP）。非 IP 路由协议包括传统的总线协议，如 DeviceNet。在 NIST 的路线图中非 IP 的路由协议的优先级要低于 IP 路由协议。

1. 测试床设计目标

ICS 安全测试床的设计是论证各种过程系统的安全应用，例如化工过程、机器人动态组装和大规模网络（例如燃气管道、输水管道和分布式智能交通系统）的分布式监视和控制。如上所述，测试床的主要目的就是论证工业控制系统安全标准的应用，比如将 NIST SP 800-82 中的保护措施应用到网络控制系统，观测系统的改进或者延迟性能。测试床也可以用来分析，如何在不影响工艺性能的前提下实施有效的安全保障。测试床的第三个目标就是测试网络攻击下测试床的可恢复能力。可恢复性是系统在网络攻击后的主要关注性能。研究机构、政府和行业能够基于此测试床对新技术进行验证分析，提高入侵检测技术，使控制过程在应对攻击时具有更强的恢复性。

2. 测试床设计架构

测试床根据仿真的工业场景分为三个部分，第一个场景是由 Downs 和 Vogel 提出的 TE 过程（Tennessee Eastman Process），这是实际化工过程制造中的经典过程。这是一个典型的开环系统。

第二个场景是机器人组装系统，通过工业机器人之间的协调工作来完成将部件在模拟的操作控制台上的移动。这是一个典型的闭环系统。

第三个场景是由范德堡大学根据与 NIST 的合作协议设计的。基本的概念包括具有大规模 SCADA 管道网络和具有分布式基础结构控制的智能交通系统。

3. TE 过程仿真

TE 过程作为连续过程模型主要有以下几点原因：①TE 模型是控制系统中的最经典的模型，平台过程的动态性比较容易理解；②这一过程必须被控制，否则其他扰动会使系统进入不稳定状态。TE 过程模型的这种内在的不稳定的开环控制在实际中被网络攻击利用就很容易能够引起人员安全、环境安全和经济损失；③这个过程是复杂的、非线性的，并且有许多其他因素控制和干扰过程的动态性。最后，TE 过程有很多现成可用的代码。

TE 过程的实际工艺流程图如图 4-18 所示。

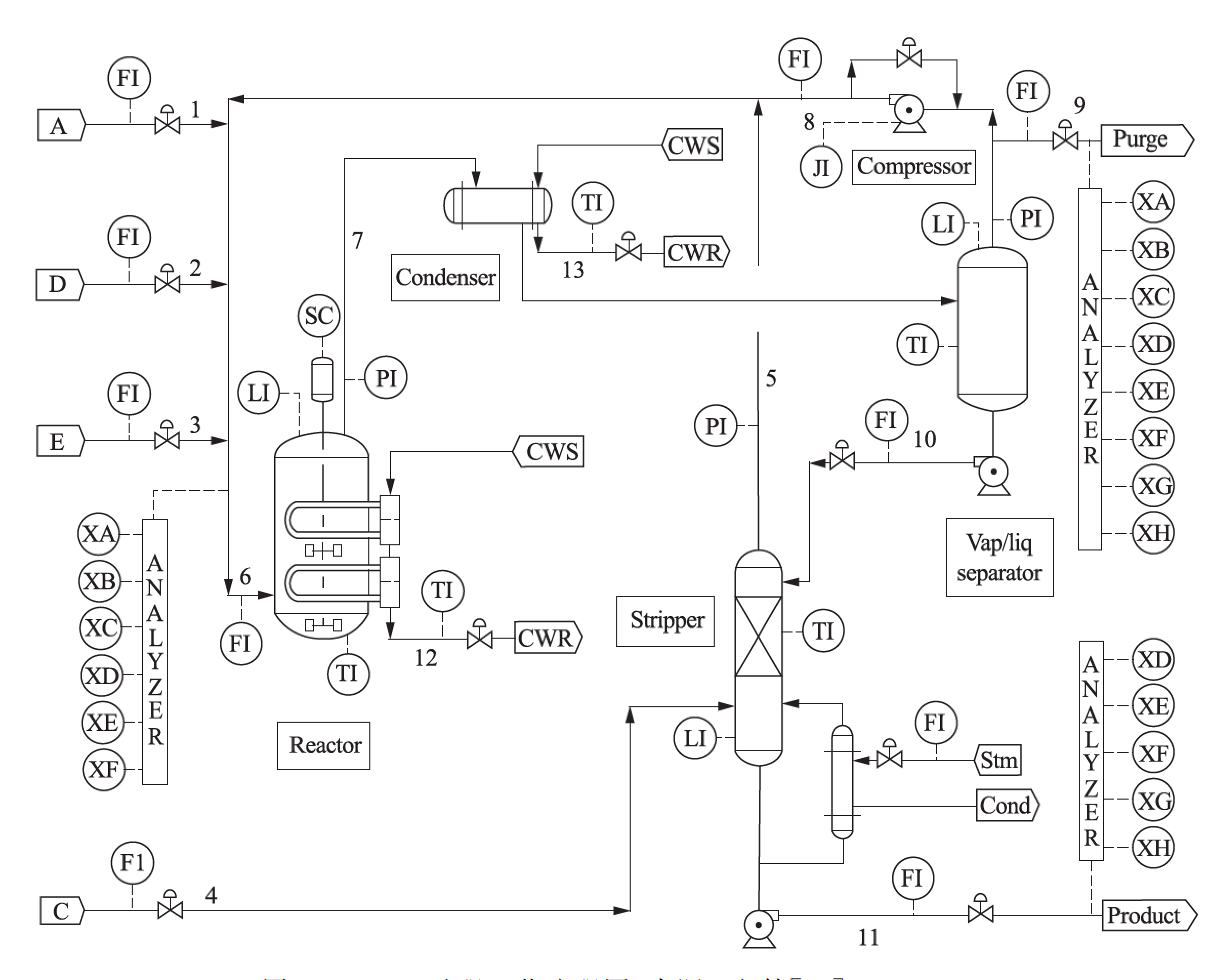


图 4-18 TE 过程工艺流程图(来源：文献[12] Figure 1)

这个过程使用四种原料 A、C、D、E，产生两种产品 G 和 H。本过程是不可逆转的和放热的，四个反应罐的反应速率是反应温度的函数。整个过程分为五个部分：反应釜、冷凝器、气液分离器、分离器和回收压缩机。

反应过程简要描述如下(参考图 4-18)：反应器中气体的反应物相结合，形

成液态产品。反应器的温度必须使用冷却水冷却进行控制。反应并不能 100% 进行,会有一些气体留存在里面。反应罐的产品进入冷凝器,将其进一步冷却为液体形式。气液分离器将未反应的气体与液体产品进行分离。未反应的气体通过离心循环压缩机送回到反应罐中。分离过程也不会 100% 进行,剩余的在汽提塔中与通过管道 4 输送的 C 进行混合,反应物 G 和 H 进一步进行精制。反应的副产物净化后通过 9 所示的清除阀。

对于 TE 过程来说,实际的网络结构图如图 4-19 所示。

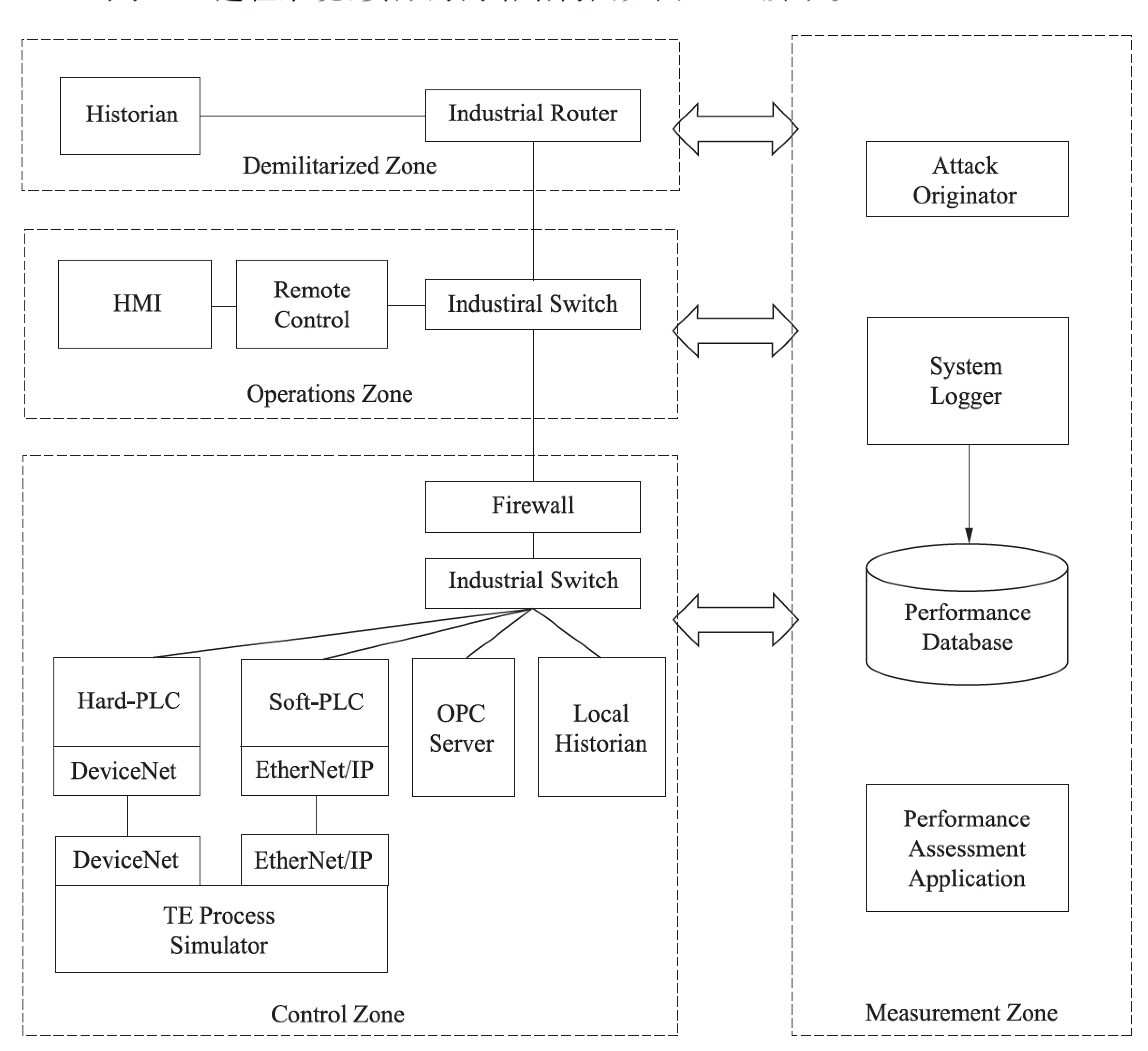


图 4-19　TE 过程网络结构图(来源:文献[12] Figure 2)

网络系统共分为三个区域:控制区域、操作区域和 DMZ 区。控制区域主管 TE 设备和控制器进程。操作区域主管数据可视化的人机界面、修改模拟设定值以及参数。DMZ 区将控制网络与办公网络隔离开,主要是使用一台历史服务器允许办公网数据进入到 TE 设备,防止未经允许的控制器状态数据进入到控制网络。

TE 设备和控制过程的状态数据都是由 OPC 服务器处理，OPC 服务器通过各种工业协议与 PLC 连接，例如不可路由的 DeviceNet 协议和可路由的 EtherNet/IP 协议。进程状态是由 PLC 传送到 OPC 服务器分配，也就是本地的历史服务器记录状态数据然后将其转发给 DMZ 区的企业历史服务器。

防火墙用在操作区域和控制区域之间，执行数据包的深度检查和设备访问授权（使用白名单机制），只要是作为 PLC 的一个网络保护机制。

此外，该模型还包含测量区域来抓取数据包，执行自定义的网络延迟，更好地仿真网路安全装置产生的延迟。

4. 智能制造中应用的协作组装机器人

机器人组装系统用于展示离散过程控制中安全措施的使用，在这个过程具有快速动作和数据量大的特点，需要确定的实时协议和基于以太网的 IP 协议的结合。网络设计图如图 4-20 所示。本系统设计使用本地局域网，控制器和机器人本体之间使用 EtherCAT 实时工业协议进行通信。

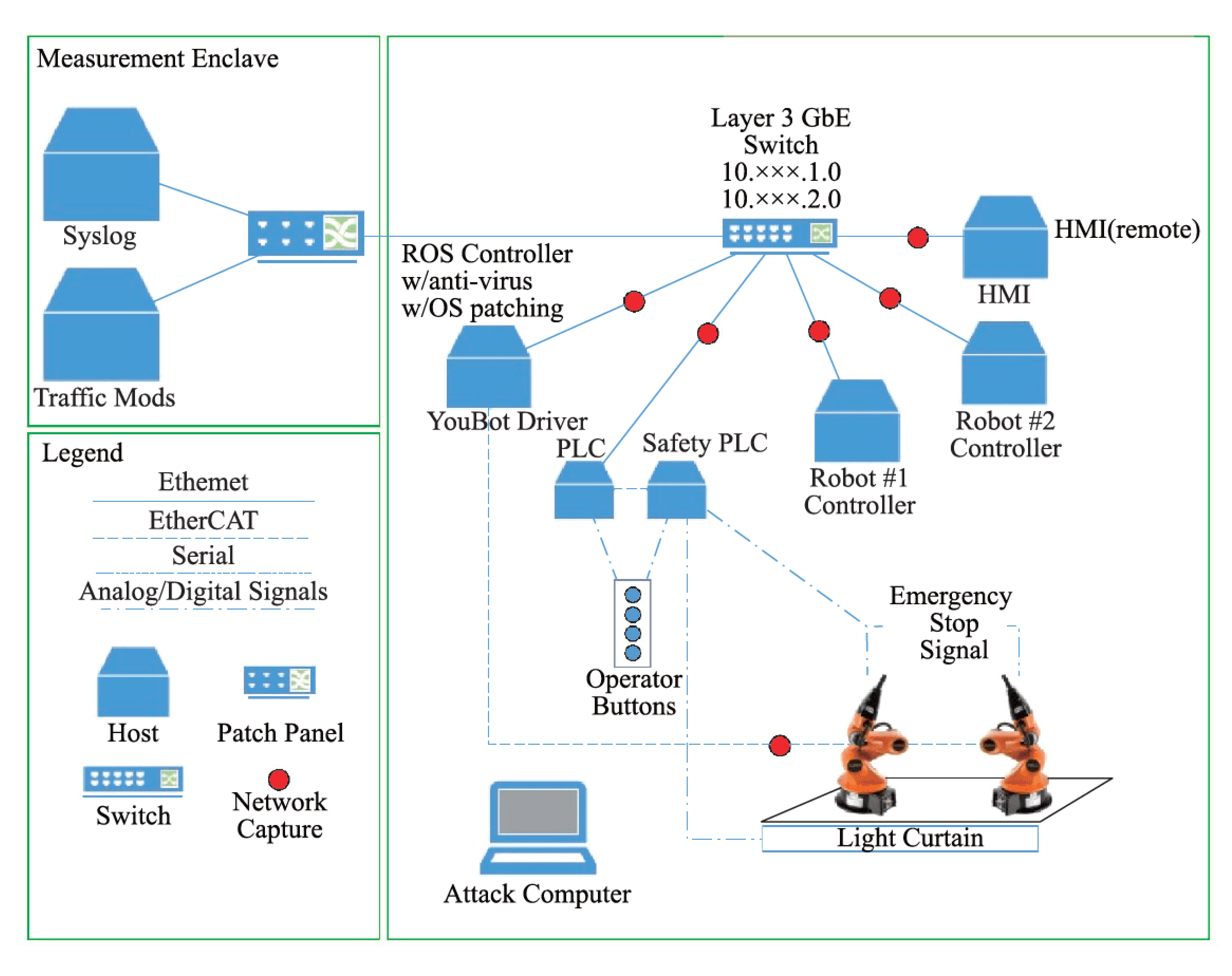


图 4-20　机器人组装系统网络架构图（来源：文献[12] Figure 6）

机器人组装系统的设计思路与 TE 过程平台的设计思路基本相同，也是将机器人系统的不同功能封装到不同的各个子模块中。三层交换机用于进行快速的网络配置。机器人组装系统与 TE 过程系统一样，也是用来验证通用安全标准的指定需求。

机器人控制器是机器人操作系统(Robot Operating System，ROS)的实现层。ROS 不是普通意义上的操作系统，而是开发机器人应用的框架。图 4-21 显示了机器人平台中 ROS 实现的节点级软件架构，所有的节点都是使用 Python 实现，软件框架也可以分为多个逻辑组。

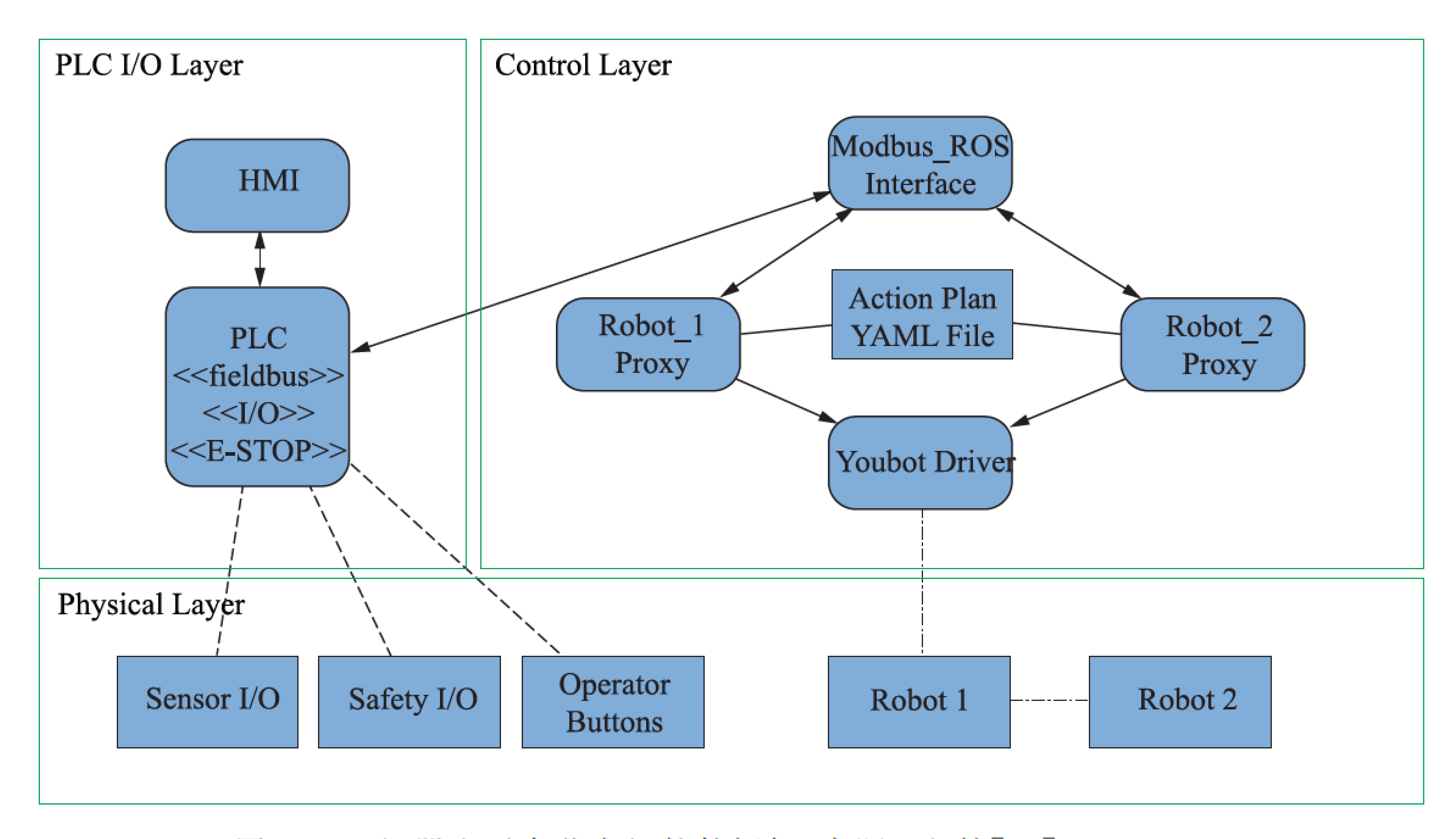


图 4-21 机器人平台节点级软件框架(来源：文献[12] Figure 12)

ROS 可以分为的关键的功能组有节点组、原理组和服务组。节点是逻辑组的基本封装，节点间通过原理组使用订阅—发布模式进行通信，通信过程是异步的。服务是以节点间异步通信的方式存在。

控制层由提供控制功能的节点组成，主要实现以下三个功能：①提供机器人具体控制的分布式控制节点；②ROS 接口节点的 Youbot 驱动；③允许 ROS 节点监视传感器、操作按钮和 PLC 状态的 Modbus 接口。

PLC I/O 层是为 ROS 和 PLC 之间连接桥梁提供服务。HMI 是当前机器人和控制系统的状态的图像化显示界面。图形界面也包括相关的控制功能，例如程序启停、系统状态指示、安全状态指示和程序选择。

当所有的一切准备完毕后，系统通过检测面板上的操作按钮来进行启动。对于每个机器人来说，都有相互间的传递和顺序传递两种工作方式。工件在进

入工作台前按顺时针顺序移动。

5. 大规模 SCADA 管道网络和具有分布式基础结构控制的智能交通系统

这个平台主要包括具有大规模 SCADA 管道网络和具有分布式基础结构控制的智能交通系统，目前还处于概念设计阶段。

6. 测试床应用

总的来说，工业控制系统的过程包括连续控制、离散控制以及混合控制三类。连续控制是指系统中的原料不能中断或者等待，离散控制是指系统的原料经常出现中断或者等待的情况，但是多数系统还是两者兼有的系统。控制系统的划分以及举例如表 4-2 所示。

表 4-2　工业过程分类

类别	过程实例
高度连续过程	• 化工生产 • 油气精炼 • 油气生产和销售 • 半导体生产 • 冶炼 • 消毒
高度离散过程	• 机器人装配 • 自动化组装 • 楼宇自动化
连续离散混合过程	• 糖果生产 • 制药 • 金属合金制造

安全指标和工艺性能指标都必须应用于工业控制系统中。工艺性能指标有吞吐量、产品质量、产品差错率和运营成本。安全指标也就是信息技术出版物（如 NIST SP 800-55 和信息技术安全评估通用标准）中公开定义的指标。

工业控制系统安全测试床用于验证 IEC62443 描述的安全需求，这些需求也反映了 NIST 800-82 的原则。IEC 系列的文档归类如图 4-22 所示。

在这些文档中 1-X 系列的文档讲述了标准的目的以及标准使用的环境，2-X 系列的文档讲述了安全需求以及 ICS 安全的实施政策和过程，3-X 系列的文档

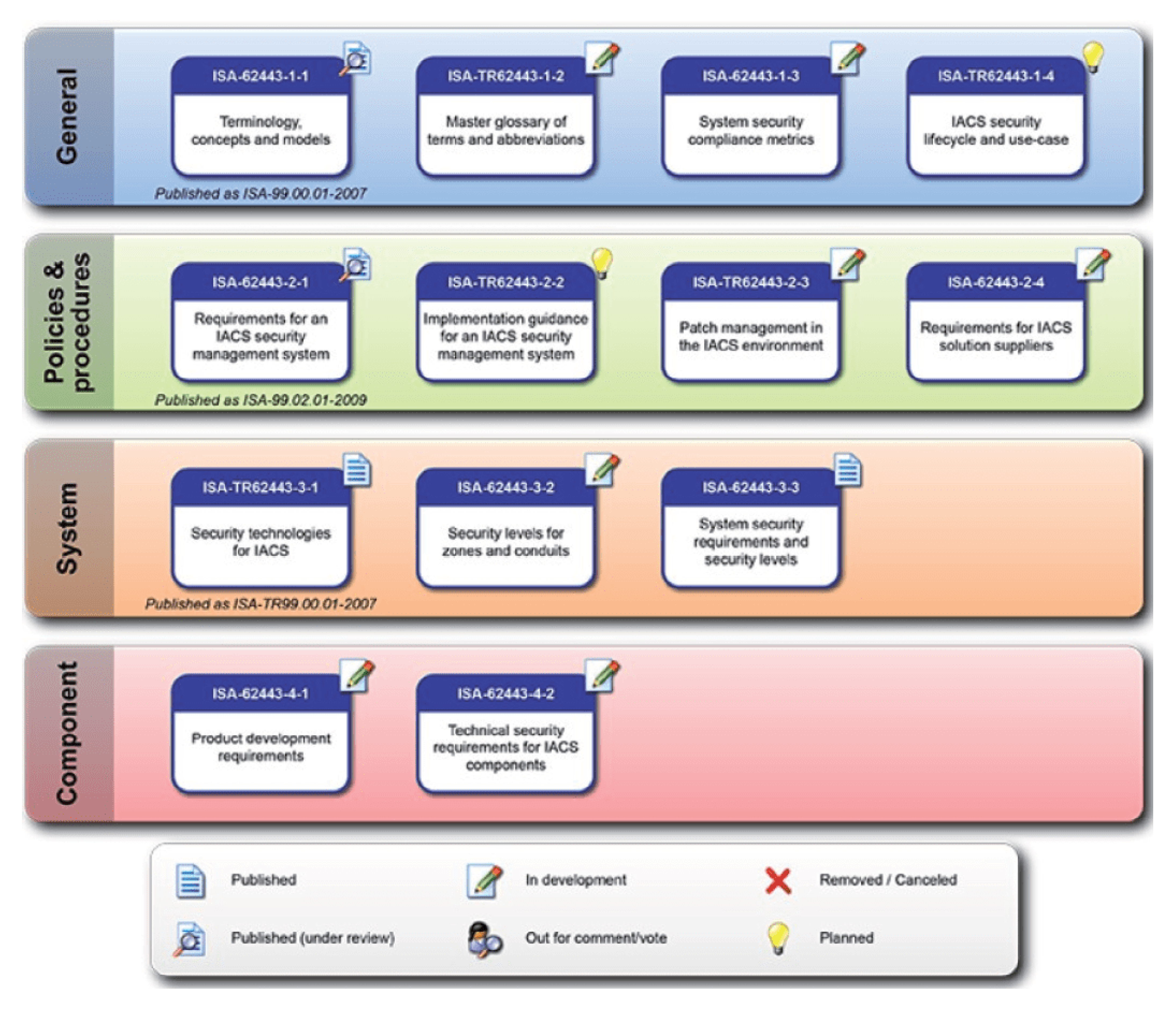


图 4-22　ISA/IEC-62443 标准文档归类(来源：文献[12] Figure 15)

讲述了系统集成的架构需求以及将安全技术应用到 ICS 集成系统中的指导方针，4-X 系列的文档讲述了生产商实现他们产品的安全需求。

表 4-3～表 4-7 是测试中使用的一些测试指标以及解释。

表 4-3　连续过程的性能指标

指标	描述
过程可用率	工业过程中正常的时间占总时间的比率
产品质量	产品的优良(废品率)或者纯度的统计数据
过程可变性	过程变量从稳定点或者设定点偏离或者振荡的数量的统计测量值
稳态误差	当系统从一个稳态过渡到新的稳态，或系统受扰动后又重新平衡后，系统出现的偏差
响应时间	控制系统从扰动到恢复正常状态的时间

续表

指标	描述
测试费用	在当前运行过程测试所需要的花费
安全系数	当检测到错误后的系统关闭时间，当涉及人身安全时特别重要
极限状态下的运行时间	在极限状态下过程控制变量时间积累的测量值
绝对误差积分(IAE)	评估系统反馈控制的通用指标
时间与绝对误差乘积的积分(ITAE)	评估系统反馈控制的通用指标

表 4-4　离散过程的性能指标

指标	描述
产品质量	产品优良或纯度的定量测量
缺陷率	由于生产过程中产品质量控制失败导致的错误的概率
单位次品数	单位范围内次品数量的统计数
过程重新启动率	在固定的时间间隔内，控制过程必须重启的次数
在线运行的变异性	命令和执行完成之间的时间统计测量值
过程持续时间	任务序列完成的时间长度，例如在机器人组装系统中的一系列的组装任务

表 4-5　测量系统性能的指标

指标	描述
易失性存储器	系统内存的利用率通常报告为 RAM 总数的百分比
非易失性存储器	系统内存的利用率通常报告为总的系统硬盘空间的百分比
CPU 利用率	总的 CPU 利用时间的百分比
I/O 读取负载	CPU I/O 信道读取的总字节数
I/O 写入负载	CPU I/O 信道写入的总字节数
扫描丢失率	当设备(如 PLC)在执行下一个控制循环前扫描变量时，在给定的时间内没有读取到的传感器的总数量

表 4-6　系统性能的标称指标

指标	描述
媒介类型	例如铜线、光纤、无线以及使用的相应协议如 CAT-6 铜线、802.11g 无线
物理信道带宽	分配给信道的全部带宽。用于无线信道比如 IEEE802.15.1 和调制的无线信道比如 Ethernet
额定信道容量	网络中发送和接收的元素的额定容量
信道编码	用于编码传输的算法或者结构，包括交错、信道编码、调制和干扰处理属性
环境特性	系统部署环境的机械、电气和电磁特性
信道压缩	传输时的数据压缩算法
额定信道的吞吐量	给定的传输或者接收设备的标称的理论吞吐量
使用的路由算法	所使用的路由算法的类型。知道路由算法对于移动自组网和满载自组网尤其有用
使用的交换算法	二层交换机所使用的算法类型
确定性边界	系统的即时约束条件

表 4-7　测量网络性能的指标

指标	描述
信息的包速率	在最高观测网络层上测量到的用于应用层的信息包速率
信息的比特速率	在最高观测网络层上测量到的用于应用层的信息比特率
原始包速率	在第二层测量到的包含开销和重试的原始包速率
原始比特速率	在第二层测量到的包含开销和重试的原始比特速率
信息延迟(分布式)	全部信息(多个数据包)在网络和网络连接中的延迟。用于在数据包重组的那层(通常是应用层)上的长数据包的测量
包延迟(分布式)	单个数据包在网络和网络连接中的延迟
包延迟抖动	测量到的一整串数据包延迟变化
处理延迟	由网络连接设备(交换机和路由器等)所引起的延迟
排队延迟	数据包在处理之前输入到队列中所需的时间
传输延迟	量子信息在传输端和接收端之间传播所需要的时间
包冲突	二层设备报告的冲突数量
包错误率	在传输层测到的数据包的错误率
包丢失率	在传输层测到的数据包的丢失率
数据包大小(分布式)	通过网络传输数据包大小的分布
探明的确定性边界	实时确定性失败的测量点

4.5 小结

本章深入分析了近年来 NIST 在工业控制安全方面所做的工作和相关成果，重点介绍了 SP 800-82《工业控制系统(ICS)安全指南》、《提高关键基础设施网络安全的框架规范》和工业控制系统网络安全性能测试床等标准文献和项目情况。

参考文献

[1] Keith Stouffer，Victoria Pillitteri，et al. Guide to Industrial Control Systems (ICS) security：Supervisory Control and Data Acquisition (SCADA) Systems，Distributed Control Systems (DCS)，and other control system configurations such as Programmable Logic Controllers (PLC). 2011. http://nvlpubs. nist. gov/nistpubs/SpecialPublications/NIST. SP. 800-82r2. pdf
[2] NIST. Framework for improving critical infrastructure cybersecurity. https://www. nist. gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214. pdf
[3] NIST. Cybersecurity for smart manufacturing systems. https://www. nist. gov/programs-projects/cybersecurity-smart-manufacturing-systems
[4] NIST. Cybersecurity for smart grid systems. https://www. nist. gov/programs-projects/cybersecurity-smart-grid-systems
[5] NIST. Smart CITIES/CPS at NIST. https://www. nist. gov/sites/default/files/documents/2017/05/09/smartcities_cps_budgetsheet. pdf
[6] NIST. Reference architecture for cyber-physical systems. https://www. nist. gov/programs-projects/reference-architecture-cyber-physical-systems
[7] NIST. Public safety communications research. http://www. nist. gov/oles/public_safety. cfm
[8] NIST Special Publication 800-39. Managing information security risk-organization，mission，and information system view. http://nvlpubs. nist. gov/nistpubs/Legacy/SP/nistspecial publication800-39. pdf
[9] NIST Special Publication 800-37. Guide for applying the risk management framework to federal information systems. http://csrc. nist. gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final. pdf
[10] ISA. NIST cybersecurity framework core：informative reference standards. https://www. americanbar. org/content/dam/aba/administrative/law_national_security/nistframework/NIST%20Cybersecurity%20Framework%20Core%20-%20ISA%2062443-2-1-2009. authcheckdam. pdf
[11] NIST. Recommended security controls for federal information systems. https://www. nist. gov/publications/recommended-security-controls-federal-information-systems-0
[12] NIST. An industrial control system cybersecurity performance testbed. 2015. http://nvlpubs. nist. gov/nistpubs/ir/2015/NIST. IR. 8089. pdf

第 5 章　美国国家科学基金会

5.1　美国国家科学基金会简介

美国国家科学基金会(National Science Foundation,NSF)成立于 1950 年,其宗旨是振兴美国的科学事业,促进美国科学事业的发展,其组织架构图如图 5-1 所示。NSF 不仅按学科建立了各种委员会,还根据研究某种特殊问题的需要,建立了一些特别委员会。NSF 主要通过发起科学与工程学研究项目,资助科学与工程学教育中的某些活动来实现其宗旨,其本身不承担任何具体的研究项目。通过对基础研究计划的资助,NSF 致力于改进科学教育、发展科学信息和增进国际科学合作等,促进美国科学的发展。基金会自 1950 年 5 月 10 日创建以来,在促进美国科学发展和培养科技人才方面做了大量工作,在国内外科技界享有很高的声誉。

NSF 主要在基础研究、科学教育、应用研究、科学政策、国际合作等方面组织开展学术研究。此外,根据国家科学基金会法,NSF 应向总统递两份报告并呈送国会。一份报告是每年一度的“国家科学基金会年度报告”(NSF Annual Report)。报告上一年度基金会的活动状况;另一份报告是两年一度的“科学指标”(Science Indictors),主要报告美国的科技现状。

从 1995 年至今,NSF 先后发布了四份战略规划报告,分别是《处于世界变幻中的美国国家科学基金会战略规划》[1]、《美国国家科学基金会〈政府业绩与成果法〉2001—2006 财年战略规划》[2]、《投资美国未来:美国国家科学基金会 2006—2011 财年战略规划》[3]和《通过发现与创新增强国力:美国国家科学基金会 2011—2016 财年战略规划》[4]。表 5-1 总结了 NSF 近年来的战略规划。

5.2　关键基础设施安全建设

2012 年 9 月 25 日,NSF 投资 5000 万美元资助了 70 余个属于 NSF“安全与可信网络空间(SaTC)”的项目,旨在提高操作系统、软件、硬件和关键基础设施

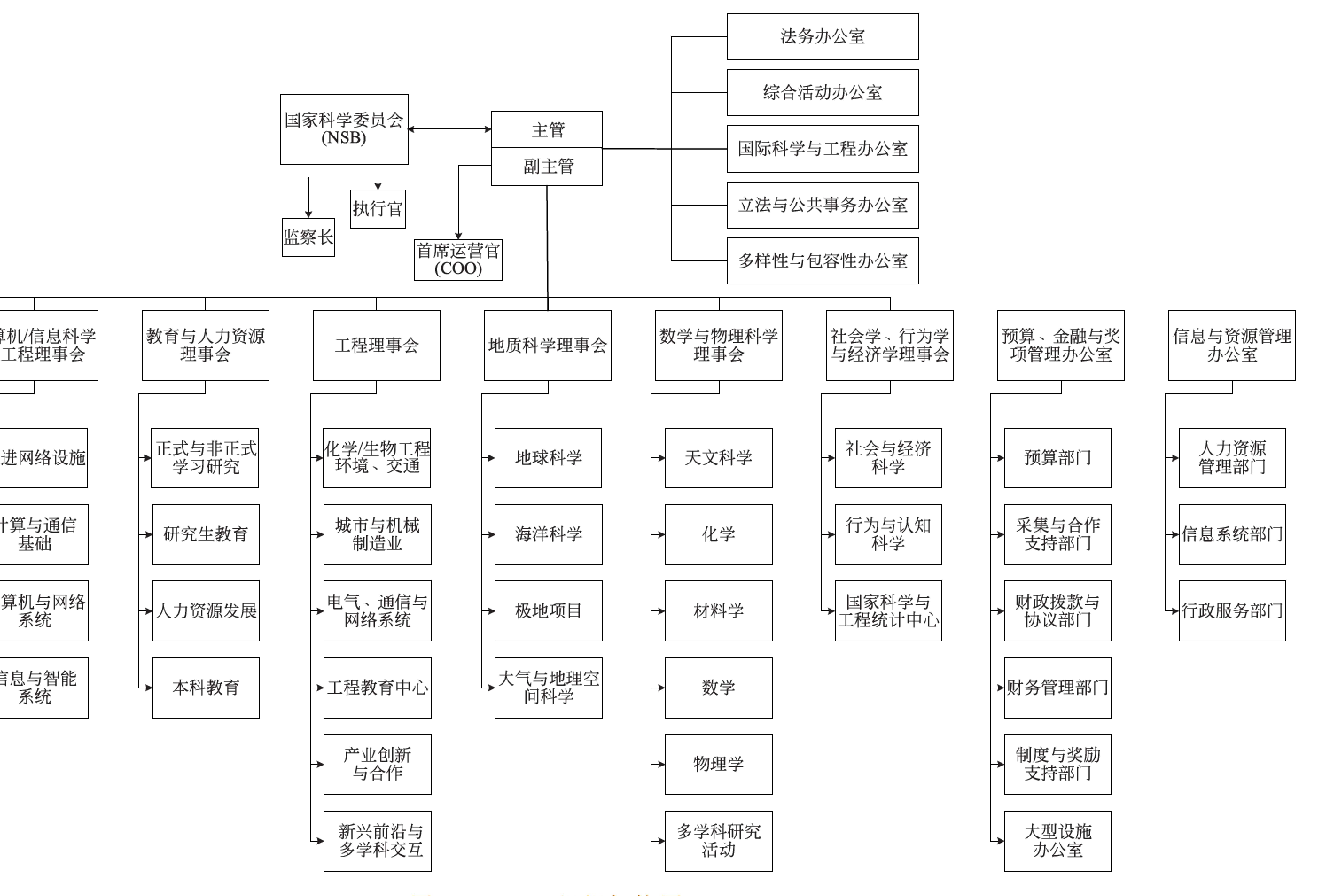


图 5-1 NSF 组织架构图

表 5-1　NSF 战略规划总览表

内容＼时间	1995—2001 年	2001—2006 年	2006—2011 年	2011—2016 年
愿景	为国家的科学、数学和工程的发展培育人才，让科学为社会服务	通过探索发现、教育学习和创新，打造美国的未来	促进探索发现、创新和教育，拓展现代知识疆域，助力未来科学和工程的发展	NSF 希冀美国能成为通过科学与工程的新观念发展自我、引领世界科研与教育的国家
战略目标	• 引领世界科学 • 加强与其他机构的合作	• 思想 • 人才 • 工具 • 组织先进性	• 探索发现 • 教育学习 • 研究基础设施 • 科研队伍	• 变革科学前沿 • 为社会的发展而创新，成为机构组织的榜样
实现方式	• 提供多样的资助模式 • 提高机构的效率和绩效 • 促进各学科智力资源的整合	• 开发智力资产 • 整合科研与教育 • 促进各方合作	• 投资未来（基础性和变革性研究、人才队伍培养、先进设备和基础设施的投资） • 整合科研与教育 • 加强国内、国际相关机构的合作	• 加强组织外合作 • 加强对项目和奖项评审过程的监督 • 组织运行以管理为导向
绩效评估		• 价值评议 • 访问专家委员会 • 咨询委员会 • 内部管理层评估	• 价值评议 • 访问专家委员会 • 咨询委员会 • 其他（完成各法案的要求、项目评估工具、组织内自我评估、NSF 亮点活动经验总结）	• 价值评议 • 访问专家委员会 • 咨询委员会 • 其他（业界专业人士和组织的建议报告、问卷调查）

的弹性，保护隐私，促进可用性，并确保从基础研究到原型部署的可信度[5]。

2015 年 9 月 24 日，美国自然科学基金会(NSF)宣布投资 4000 万美元启动自然灾害工程基础设施研究(Natural Hazards Engineering Research Infrastructure, NHERI)项目，以更好地抵御地震、风灾和水灾带来的影响。NHERI 主要涉及网络基础设施和实验设备[6]。

在关键基础设施领域，为了提高美国关键基础设施的恢复力并增强其服务功能，2015 年 9 月 14 日，NSF 宣布投入 2000 万美元用于研究如何改善基础设施系统，即"重要基础设施和过程的弹性相互依赖"(Critical Resilient Interdependent Infrastructure Systems and Processes, CRISP)。该项目的目标是从物理到网络应急响应角度来开展基础设施设备和系统的基础研究，对基础设施进行新的理解和认识，结合建模和智能技术的进步，不断提高系统的韧性，在创造更高的恢复能力方面得以实现突破性的发现[7,8]。

5.3 CRISP 项目介绍

该项目在 2015 年资助了 12 个课题。CRISP 的研究者将从设计和性能评估的角度出发，研究在自然灾害、技术或人为误操作等故障或者系统失效的情况下，如何保证这些存在相互依赖关系的关键基础设施系统仍能够快速恢复并正常运行。这些研究工作将促进关键基础设施系统的更新换代和创新设计与实验。通信、电力和水能源的供应，以及其他社区基础设施的支持服务能力将被大大加强，而且这些系统的运行也将变得更加稳定持续和安全。

5.3.1 总体目标

研究目标：

(1) 在运行与服务方面，为基础设施的设计与操作提供新的技术路径、解决方案。

(2) 增强对相互依赖的关键基础设施(Interdependent Critical Infrastructure, ICI)系统与过程的认识与设计，为任何原因导致的系统中断/失败/干扰提供必要的应急物资与服务。

(3) 为 ICI 的革新提供理论支撑，安全、有效地扩大 ICI 所能提供的服务范围。

(4) 在 ICI 现有的产品与服务方面，不断提高其有效性、可靠性及运行效率。

研究内容：

（1）通过提出新的知识、方法、解决方案来增强 ICI 系统的弹性、性能、应急响应能力。

（2）为 ICI 的系统、流程与服务创建框架与多学科模型，对复杂的行为进行分析预测，能够实时控制、动态适应、重新配置，响应系统和政策的变化。

（3）为物理、网络、社会行为和经济等 ICI 元素开发框架，以对各基础设施间的相互依赖关系进行分析。

（4）对组织、社会、心理、法律、经济、技术等方面的障碍进行分析理解，为 ICI 创建识别策略，提高 ICI 网络安全攻击应对能力。

5.3.2　课题介绍

CRISP 项目课题类别分成 Ⅰ 类和 Ⅱ 类两种[9]，其中 Ⅰ 类课题资助事件为 3 年，最高 50 万美元，Ⅱ 类课题资助事件为 3～4 年，最高为 100 万～200 万美元。两类课题一共资助了 12 个课题。课题基本信息如表 5-2 所示。

表 5-2　CRISP 课题基本信息表

序号	项目名称	项目周期	经费/美元	负责人	承担单位
1	可恢复力分析：利用数据驱动的方法，增强相互依存网络的弹性	2015.10.15—2018.9.30	1 381 958.00	Kash Barker (kashbarker@ou.edu)	University of Oklahoma Norman Campus
2	对相互依赖系统进行概率性的弹性评估	2015.9.1—2018.8.31	1 903 209.00	Paolo Bocchini (paolo.bocchini@lehigh.edu)	Lehigh University
3	对几十年来针对关键基础设施的攻击进行分析学习	2016.1.1—2018.12.31	98 357.00	Ross Baldick (baldick@ece.utexas.edu)	University of Texas at Austin
4	人口基础设施的联系：开发一个基于数据流的多样化方法，对 ICI 系统的中断响应进行分析	2016.1.1—2018.12.31	150 000.00	Guangqing Chi (gchi@psu.edu)	Pennsylvania State Univ University Park

续表

序号	项目名称	项目周期	经费/美元	负责人	承担单位
5	通过进化来改革：改善社会与电力的交互作用的控制方法	2015.9.15—2018.8.31	1 409 942.00	Andrea Mammoli (mammoli@unm.edu)	University of New Mexico
6	基于仿真的假设检验，对使用分布式优化与自然语言处理的社会技术社区进行分析	2015.10.1—2019.9.30	1 208 929.00	Scott Miles (milessb@uw.edu)	University of Washington
7	开发相互依存的电气和云服务，建立可持续、可靠、开放的智能电网	2015.9.15—2018.8.31	1 499 988.00	Manuel Rodriguez-Martinez(manuel.rodriguez7@upr.edu)	University of Puerto Rico Mayaguez
8	多尺度下基础设施在突发事件中的交互：沿海防洪、交通和治理网络	2015.10.1—2019.9.30	1 879 485.00	Mark Stacey (mstacey@Berkeley.EDU)	University of California-Berkeley
9	弹性智慧城市	2016.1.1—2019.12.1	1 100 000.00	Walid Saad (walids@vt.edu)	Virginia Polytechnic Institute and State University
10	建立多尺度建模框架，对弹性、相互依赖的关键基础设施系统进行评估和控制	2015.9.1—2018.8.31	499 920.00	Iris Tien (itien@ce.gatech.edu)	Georgia TechResearch Corporation
11	弹性、网络化的电能和配水系统基础设施：在极端超级干旱场景下进行建模与控制	2015.8.1—2018.7.31	1 478 907.00	Vijay Vittal (vijay.vittal@asu.edu)	Arizona State University
12	改善多尺度相互依赖的关键基础设施的弹性	2015.9.1—2018.8.31	500 000.00	Quanyan Zhu (quanyan.zhu@nyu.edu)	New York University

1. 利用数据驱动的方法，增强相互依存网络的弹性[10,11]

（Resilience Analytics：A Data-Driven Approach for Enhanced Interdependent Network Resilience）

负责人：Kash Barker（University of Oklahoma（OU））

参与人：James Lambert（University of Virginia），Laura McLay（University of Wisconsin-Madison），Charles Nicholson（University of Oklahoma（OU）），Jose Ramirez-Marquez（Stevens Institute of Technology）

NSF 提供资金：$1 381 958.00

课题类型和时间周期：CRISP Ⅱ类，2015.10.15—2018.9.30

课题简介：近几年由自然灾害所引发的具有连带效应的破坏性事件给管理安全事件和编制应急预案提出了新的挑战。其中，具有连带效应的安全事件会给相互依存的不同系统和网络带来致命的破坏。理解这些系统之间的关联关系，找出可能存在安全隐患的薄弱衔接环节，并进行重点防护，将有助于提高系统对安全事件的应急响应和恢复能力。目前，社交媒体提供了社区网络（如亲朋好友、邻居），物理基础设施网络（如交通、电网），应急服务网络（如应急响应服务人员、修复人员）等方面的海量数据。这些数据有利于研究人员分析理解不同系统和网络之间的相互依赖关系，进而研究如何消除不同系统和网络之间的脆弱性，提高系统和网络的恢复力。CSIRP 项目整合了工程，计算机科学和社会科学等多个学科专业科研人员，以不同视角进行合作研究，通过数据驱动的方式来提高系统和网络的恢复力。本课题拟研究如何利用数据驱动的方式来理解系统弹性的含义。即在自然灾害事件发生之前、之中和之后，统计分析网络和系统的运行状态和行为模式；更有效地解决网络和系统的脆弱性问题，当自然灾害事件发生后，提高网络和系统的应急响应和恢复能力。

本课题有两个研究内容。

（1）创建一个关于基础设施网络，基础设施网络提供服务的社区网络和应急响应服务网络之间相互依赖性的网络模型。本项目将研究社区网络恢复力和基础设施网络性能之间的功能关系。

（2）将研究内容一所建立的网络模型与社区网络数据综合起来，建立一个更有助于理解和规划网络和系统的恢复力的数据分析框架。

2. 对相互依赖系统进行概率性的弹性评估[12]

（Probabilistic Resilience Assessment of Interdependent Systems）

负责人：Paolo Bocchini（Lehigh University）

参与人：Brian Davison，Alberto Lamadrid，Richard Sause and Lawrence Snyder

NSF 提供资金：$1 903 209.00

课题类型和时间周期：CRISP Ⅱ类，2015.9.1—2018.8.31

课题简介：当破坏性的极端自然灾害事件（如地震或严重的风暴）发生之后，受影响地区的基础设施系统的应急和恢复直接决定了社会经济的复苏和发展。电力和供水系统、交通网络、通信系统和关键建筑在应对灾害的过程中担任着主要角色。如果这些基础设施无法从中断中及时恢复的话，那么社会和经济就会遭受巨大的损失。本课题汇集了土木工程、系统工程、计算机科学、经济学、城市规划和政策制定等不同领域的科研学者。本课题目的是当发生复杂极端事件后，在不确定性条件下，通过综合考虑独立基础设施系统模型和不同系统相互依赖性模型特点，建立一个衡量相互依赖系统恢复力的评价框架。

本课题拟搭建一个称为"PRAISys"（Probabilistic Resilience Assessment of Interdependent Systems，相互依存的系统概率性评估）的平台，通过概率分析方法，分析相互依赖模型的所有影响因素，分析模型的不确定性并加以分类，利用数学和计算工具来捕捉模型的特点。本课题拟通过搭建、验证和分析 PRAISys 平台，为基础设施网络设计和管理提供更有效的分析方法，以此来应对极端事件和系统故障问题，防止发生灾难性的人身伤亡，防止极端事件给社会经济和环境带来长久的破坏影响。

3. 对几十年来关于关键基础设施的攻击进行分析学习[13]

（Lessons Learned from Decades of Attacks against Critical Interdependent Infrastructures）

负责人：Ross Baldick（University of Texas at Austin）

NSF 提供资金：$98 357.00

课题类型和时间周期：CRISP Ⅰ类，2016.1.1—2018.12.31

课题简介：相互依赖的关键基础设施（如电网、供水和交通等大规模系统），为现代生活提供最基本的日常服务。之前对这些基础设施的保护都集中在防止意外事故造成的物理破坏上，但是现在对于基础设施的防护则不仅关注物理防护，而且还注重网络安全防护。本课题针对哥伦比亚 50 年以来关键基础设施遭受的攻击事件进行分析，并总结成功实践和经验教训，汇总技术解决方案。通过开展本项目，国家能够更好地理解威胁的性质，并且公共和私营部门也能够更好地开展态势感知与安全保护工作。

4. 人口基础设施的联系：开发一个基于数据流的多样化方法，对 ICI 系统的中断响应进行分析[14]

(Population-Infrastructure Nexus: A Heterogeneous Flow-Based Approach for Responding to Disruptions in Interdependent Infrastructure Systems)

负责人：Guangqing Chi (Pennsylvania State University)

NSF 提供资金：$ 150 000.00

课题类型和时间周期：CRISP Ⅰ类，2016.1.1—2018.12.31

课题简介：降低关键基础设施系统的不稳定性和脆弱性，有助于提高整个社会的运行效率与弹性。灾难性事件(如 2003 年的东北部大停电和 2012 年飓风桑迪)可以给 ICI 系统(如电力网络、燃料供应和运输系统)带来严重的破坏。这些破坏给基础设施系统的各个组件的应急响应能力提出了严峻的挑战。而且，当受破坏地区的人口发生剧烈变化时(如地区短时间内聚集了许多人)，基础设施系统的应急响应恢复就会变得更有难度。本课题的目的就是在各种破坏(包括操作的不确定性和灾难性的破坏)情况下，提高 ICI 系统的弹性。

本课题研究目的是设计一个分布式异构的基于流程的建模框架，以量化评估 ICI 系统和人口群体之间复杂的依赖关系。框架也将用来分析短期人口流动行为和长期的人口发展对基础设施的影响。

本课题拟实现以下目标：

(1) 量化不同人口群体与多个基础设施的关联关系。

(2) 描述相互连接的不同基础设施系统之间的依赖关系。

(3) 人口与不同的基础设施通过网络平台进行人机交互，形成一个自组织的分布式系统，对该系统中的人口-基础设施系统进行建模和优化分析。

(4) 分析对人口-基础设施系统模型的均衡点和稳定性。

本课题预期成果包括：

(1) 通过建立一个基于异构网络数据流的建模方法来定义不同相互依赖基础设施系统的动态变化和均衡特性。

(2) 基于建立的人口-基础设施系统模型，提供分析人口群体和基础设施系统之间的双向影响关系功能。

(3) 建立的人口-基础设施系统模型将融入基于自组织群体智能的分布式网络通信平台中，以此支持人口和基础设施系统交换信息，进而实现行动自治化。

5. 通过进化来改革:改善社会与电力的交互作用的控制方法[15]

(Revolution through Evolution: A Controls Approach to Improve How Society Interacts with Electricity)

负责人:Andrea Mammoli (University of New Mexico (UNM))

参与人:Majeed Hayat and Francesco Sorrentino (University of New Mexico (UNM))

NSF 提供资金:$1 409 942.00

课题类型和时间周期:CRISP Ⅱ类,2015.9.15—2018.8.31

课题简介:该课题旨在研究与电网的快速发展相适应的高度分布式基础设施中的相关挑战问题。本研究的重点是配电馈线的变换,具体范围包括为客户提供电力,建立分布式微型电网实体,积极管理本地电能的生产、存储和使用。分布式微型电网分布结合了传统电网的优势和新兴的分布式技术的优势。该项目将针对发电和交付、信息流动、市场规划和人类行为等因素来建立基于社会与电力交互作用的控制模型。基于建立的模型,政策制定者可以规划由分布式微型电网来实现清洁能源的过程。

本课题拟使用哈密顿表面成形功率流控制理论,达到一个最优带宽、存储性能和信息设计的非线性控制器,以此检测恶意篡改信息流行为。在紧急系统动力学方面,本课题拟使用动态复杂网络理论,探索限制人类行为和市场稳定性的函数设计。最后,在如何增强可控性的影响配电系统鲁棒性的大型"能源-信息-社会"网络中,本课题拟使用相互依存的马尔可夫链模型分析。

6. 基于仿真的假设检验,对使用分布式优化与自然语言处理的社会技术社区进行分析[16]

(Simulation-Based Hypothesis Testing of Socio-Technical Community Resilience Using Distributed Optimization and Natural Language Processing)

负责人:Scott Miles, Mehran Mesbahi (University of Washington) and Noah Smith (Carnegie Mellon University)

参与人:Leonardo Duenas Osorio (Rice University)

NSF 提供资金:$1 208 929.00

课题类型和时间周期:CRISP Ⅱ类,2015.10.1—2019.9.30

课题简介:本课题有三个主要研究目标:

(1) 系统地思考关键基础设施的社会和技术系统。

(2) 建立计算机仿真模型来探索关键基础设施性能。

(3) 测试关键基础设施的韧性,以支持社会技术社区的各种需求。

关键基础设施(如电力、制造、金融系统)是社会功能和社区健康的核心单元。本课题拟通过改进关键基础设施的设计和管理方法,提高基础设施在自然灾害和人为破坏事件中的系统弹性。本课题拟重点关注不同基础设施的社会和技术关系,深入研究社会因素对关键基础设施的影响,以及关键基础设施在促进社区发展过程中所发挥的作用。课题组拟使用自然语言处理(natural language processing,NLP)来分析文本数据,描述关键基础设施性能和社会适应力,以及基础设施技术与社会之间的关系。

7. 融合电气和云服务,建立可持续、可靠、开放的智能电网[17]

(Interdependent Electric and Cloud Servies for Sustainable, Reliable, and Open Smart Grids)

负责人:Rajiv Ramnath

参与人:Manuel Rodriguez-Martinez, Marla Perez-Lugo, Fabio Andrade, Rafael Rodriguez, Efrain O'Neill-Carrillo

NSF 提供资金:$1 499 988.00

课题类型和课题周期:CRISP Ⅱ类,2015.9.15—2018.8.31

课题简介:在本课题中为智能电网建立一套电力和云服务相互交融的模型,这种交融模型使得电力系统和云协同互动,从而帮助管理智能电网。所有的电力服务(如能源、存储、计费)会作为基于 REST 的云服务向用户开放,使得电力供应商和用户可以使用和订阅电力服务,收集操作数据和用户反馈,并且支持分析预测电力需求。微型电网和可再生能源系统是这个框架的重要组成部分,它们使模块化的电网变为独立或半独立的子系统。研究小组将开发方法可靠的电力微型电网映射到电力服务,可以迅速把在线弥补发电容量或获得更多廉价的能源。

“微型智能电网”系统的主要挑战对可再生能源的可用性进行预测,通过开发太阳能和风能产出评估服务的跟踪框架,以及提高当地传感器的测定要求,以此改善短期预测服务。团队将社会认可的模型应用到智能电网的开发、实施、管理和评价当中,以此为服务商与用户提供一套可持续、可靠、开放的智能电网系统管理和考核。

8. 多尺度下基础设施在突发事件中的交互:沿海防洪、交通和治理网络[18]

(Collaborative Research: Multi-Scale Infrastructure Interactions with Intermittent Disruptions: Coastal Flood Protection, Transportation and Governance Networks)

负责人:Bruce K. Hamilton

参与人:Mark Lubell, Davis

NSF 提供资金:$575 000.00

课题类型和课题周期:CRISP Ⅱ类,2015.10.1—2019.9.30

课题简介:对沿海社区洪水威胁的理解需要整合气候科学、沿海海洋和水动力学、交通工程、计划和政治科学。在此 CRISP 项目中,需要对这些学科进行整合,以此定义网络结构。目的是在沿海区域洪水事件中研究基础设施和治理网络在多尺度下的相互作用。通过使用最先进的水动力模型,对由于海平面上升、海洋水位波动(包括潮汐、降水和径流)造成的洪水事件进行预测,并以此决定基础设施的位置,建立交通基础设施与区域治理网络。

本课题对三个基础设施网络之间的交互(海岸线、运输和治理)进行定量分析,建立拓扑结构和数据流。通过研究基础设施系统中沿海洪灾的现实问题,从而对沿海防洪、交通和治理网络的建立与决策进行指导。

9. 弹性智慧城市[19]

(Collaborative Research: Towards Resilient Smart Cities)

负责人:Rajiv Ramnath

参与人:Narayan Mandayam, Arnold Glass and Janne Lindqvist, Rutgers University at New Brunswick

NSF 提供资金:$916 000.00

课题类型和课题周期:CRISP Ⅱ类,2016.1.1—2019.12.31

课题简介:实现真正的智能城市是未来十年内最紧迫的技术挑战之一。这一愿景的实现需要协同集成的物理-网络系统,如智能交通、无线通信系统、水网、电网等集成到一个统一的智能城市中去。但是这会存在很大的隐患,为了应对日常运作、自然灾害和恶意攻击等可能造成的系统故障,研究将引入一个基本分析框架,利用城市 CIs 之间的协同效应产生的弹性资源管理计划认识和技术。此框架通过结合跨学科领域研究,有如下一系列进展:

(1) 通过严谨的数学工具(图论工具、力量指数、机器学习和随机空间模型等)方式,描述 ICI 之间的相互依赖关系;

（2）通过使用弹性的资源管理机制和先进的框架，优化因面临不同智能水平代理的 CI 资源的管理；

（3）智慧城市居民和 CIs 之间信任关系的行为模型；

（4）为影响用户的基础设施系统提供指导，提高基础设施的弹性；

（5）对大规模智能城市进行模拟，并进行现实的实验，形成理论与实践之间的桥梁。

10. 建立多尺度建模框架，对弹性、相互依赖的关键基础设施系统进行评估和控制[20]

（Multi-Scale Modeling Framework for the Assessment and Control of Resilient Interdependent Critical Infrastructure Systems）

负责人：M. Mimi McClure

参与人：Iris Tien（Georgia Institute of Technology），Seymour Goodman and Calton Pu（Georgia Institute of Technology）

NSF 提供资金：＄499 920.00

课题类型和课题周期：CRISP Ⅰ类，2015.9.1—2018.8.31

课题简介：本课题将采取多学科交叉的方法，结合工程计算和相关的政策来创建一个强大的利益驱动模型框架，并多尺度和以跨数据源的角度去刻画 ICIs（interdependent critical infrastructures），以此来评估基础设施的现状，对其性能和可靠性进行预测。ICIs 对我们的社会、健康、安全和我们的国家安全十分重要。这些系统由许多相互依赖的组件构成。此外，这些系统是相互依存的，一个系统的性能依赖于一个或多个其他系统的性能。这让 ICIs 容易受到各种各样的危害，包括自然的和人为的。

本课题将研究如何提高这些系统的弹性，研究人员将研究 ICIs 系统，特别是交通、电力、通信基础设施，并在城市与农村这两个不同环境中应用 ICIs 框架，并进行评估，使弹性基础设施管理系统能够反应、适应，甚至主动采取预防行动，以应对即将到来的灾难。

此课题的研究结果也将集成到更加广阔的课堂教学和教育科研领域的活动，培养下一代在关键基础设施恢复起着重要作用的科学家、工程师和决策者，以及开发用来实现弹性系统和快速恢复的新的多学科方法和各种工具。

11. 弹性、网络化的电能和配水系统基础设施：在极端超级干旱场景下进行建模与控制[21]

（Resilient Cyber-Enabled Electric Energy and Water Infrastructures: Modeling and Control under Extreme Mega Drought Scenarios）

负责人：Bruce K. Hamilton

参与人：Vijay Vittal (Arizona State University), Virginia Kwan, Larry Mays and Junshan (Arizona State University)

NSF提供资金：$1 478 907.00

课题类型和课题周期：CRISP Ⅱ类，2015.8.1—2018.7.31

课题简介：弹性、可靠和高效的关键基础设施对现代社会的繁荣进步至关重要。电网和水利系统都是关键基础设施，它们是由大量的传感器、通信资源、控制和信息系统组成的高度自动化和相互依存的系统网络。

该课题将开发一个基于两个ICI系统（电力系统与供水系统）的数学模型，并识别两个系统之间的相互依赖关系。研究的总体目标是将相互依赖但独立运营的基础设施系统，通过有效的信息交换，使其可以对极端场景下可能出现的情况进行分析处理。包括以下研究和教育任务：

(1) 基于系统动力学的数学模型开发相互依赖的基础设施，包括电力基础设施、水利基础设施，识别其相互依赖关系，对相互依赖的系统进行模拟。

(2) 极端的情况下，建立社会/行为模型应急选择和分析消费者需求的商品，提供在极端的情况下的基础设施行为模型，相互依赖系统的风险评估和应急选择极端的场景，建立在极端的情况下和相关的突发事件分析模型。

(3) 对部署了网关中间件的网际网路基础设施信息系统进行优化，中间件开发和建模，实现信息和控制的共享。

12. 改善多尺度相互依赖的关键基础设施的弹性[22]

(Reductionist and Integrative Approaches to Improve the Resiliency of Multi-Scale Interdependent Critical Infrastructure)

负责人：Chu-Hsiang Chang

参与人：Quanyan Zhu (New York University), Nasir Memon, Kaan Ozbay and Rae Zimmerman (New York University)

NSF提供资金：$500 000.00

课题类型和课题周期：CRISP Ⅰ类，2015.9.1—2018.8.31

课题简介：目前，关键基础设施的发展日趋多元化，相互联系越来越紧密。由于网络-物理、地理、供需关系、人机交互等因素造成的基础设施之间的相互依赖关系也日趋复杂。该课题着重于研究这四种基本类型相互依赖关系的特点，而一体化方法使用它们作为构建块，并以此建立一个整体的网络框架来再现基础设施系统的相互依赖关系。

这种自底向上的方法提供了一种系统的方法来生成一个集成和多尺度系统的视图系统，识别和定量表征通过反馈回路的相互依赖关系。这个项目的总体目标是提高相互依赖的基础设施的弹性，使其能够在一个可接受的时间和成本内，从破坏性事件和干扰中恢复。

5.4　小结

本章介绍了美国国家自然基金在关键基础设施安全方面设立的科研项目，首先以“重要基础设施和过程的弹性相互依赖”项目为例，介绍了美国国家自然基金在该领域的科研布局。然后分别介绍了“重要基础设施和过程的弹性相互依赖”项目下的 12 个课题的基本情况。

参考文献

[1] NSF. NSF in a changing world: The National Science Foundation's strategic plan. https://www.nsf.gov/pubs/1995/nsf9524/contents.htm

[2] NSF. NSF GPRA strategic plan FY 2001—2006. http://www.nsf.gov/pubs/2001/nsf0104/nsf0104.doc

[3] NSF. Investing America's future: National Science Foundation Strategic Plan FY 2006—2011. http://www.nsf.gov/pubs/2006/nsf0648/NSF-06-48.pdf

[4] NSF. Empowering the nation through discovery and innovation: NSF strategic plan for FY 2011—2016. http://www.nsf.gov/news/strategicplan/nsfstrategicplan_2011_2016.pdf

[5] 中国科学院信息化工作网. NSF 资助保护美国网络空间的项目. http://www.ecas.cas.cn/xxkw/kbcd/201115_91634/ml/xxhzlyzc/201210/t20121016_3659352.html

[6] 中国科学院信息化工作网. NSF 投 4000 万美元建设自然灾害工程研究基础设施. http://www.ecas.cas.cn/xxkw/kbcd/201115_118276/ml/xxhjsyjcss/201510/t20151019_4440695.html

[7] 中国科学院科技战略咨询研究院. 美国 NSF 加强资助生物多样性和城市发展及灾害等领域. http://www.casisd.cn/zkcg/ydkb/kjqykb/2015/201511/201703/P020170328555526946576.pdf

[8] NSF. NSF invests $20 million to enhance resilience of critical infrastructure. https://www.nsf.gov/news/news_summ.jsp? cntn_id=136266

[9] NSF. Critical resilient interdependent infrastructure systems and processes (CRISP) at the National Science Foundation (NSF). http://www.nsf.gov/eng/cmmi/documents/CRISP_Webinar_Jan_22_2015.pdf

[10] NSF. CRISP Type 2/collaborative research: a data-driven approach for enhanced interdependent network resilience. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1541165
[11] Analytics Lab. Resilience analytics: a data-driven approach for enhanced interdependent network resilience. http://oklahomaanalytics.com/research/
[12] NSF. Probabilistic Resilience Assessment of Interdependent Systems (PRAISys). http://www.nsf.gov/awardsearch/showAward? AWD_ID=1541177
[13] NSF. Lessons learned from decades of attacks against critical interdependent infrastructures. https://www.nsf.gov/awardsearch/showAward? AWD_ID=1541159
[14] NSF. Population-infrastructure Nexus: a heterogeneous flow-based approach for responding to disruptions in interdependent infrastructure systems. https://www.nsf.gov/awardsearch/showAward? AWD_ID=1541136
[15] NSF. Revolution through evolution: a controls approach to improve how society interacts with electricity. http://www.nsf.gov/awardsearch/showAward? AWD_ID=1541148
[16] NSF. Simulation-based hypothesis testing of socio-technical community resilience using distributed optimization and natural language processing. http://www.nsf.gov/awardsearch/showAward? AWD_ID =1541025
[17] NSF. Interdependent electric and cloud servies for sustainable, reliable, and open smart grids. http://www.nsf.gov/awardsearch/showAward? AWD_ID=1541106
[18] NSF. Collaborative research: multi-scale infrastructure interactions with intermittent disruptions: coastal flood protection, transportation and governance networks. http://www.nsf.gov/awardsearch/showAward? AWD_ID=1541181
[19] NSF. Collaborative research: towards resilient smart cities. http://www.nsf.gov/awardsearch/showAward? AWD_ID=1541105
[20] NSF. Multi-scale modeling framework for the assessment and control of resilient interdependent critical infrastructure systems. http://www.nsf.gov/awardsearch/showAward? AWD_ID=1541074
[21] NSF. Resilient Cyber-enabled electric energy and water infrastructures: modeling and control under extreme mega drought scenarios. http://www.nsf.gov/awardsearch/showAward? AWD_ID=1541026
[22] NSF. Reductionist and integrative approaches to improve the resiliency of multi-scale interdependent critical infrastructure. http://www.nsf.gov/awardsearch/showAward? AWD_ID=1541164

第 6 章　美国国防高级研究计划局

6.1　美国国防高级研究计划局简介

隶属于美国国防部的美国国防高级研究计划局（Defense Advanced Research Projects Agency，DARPA）成立于 1958 年 2 月，主要针对中、远期国家安全需求来研制具有军事价值的前沿高新技术，并为军方的重大预研项目工作提供技术指导和管理。

DARPA 的组织架构如图 6-1 所示。在国防部领导下的 DARPA 局长办公室管辖着生物技术、国防科学、信息创新、微系统技术、战略技术、战术技术、行政和航空航天项目办公室。

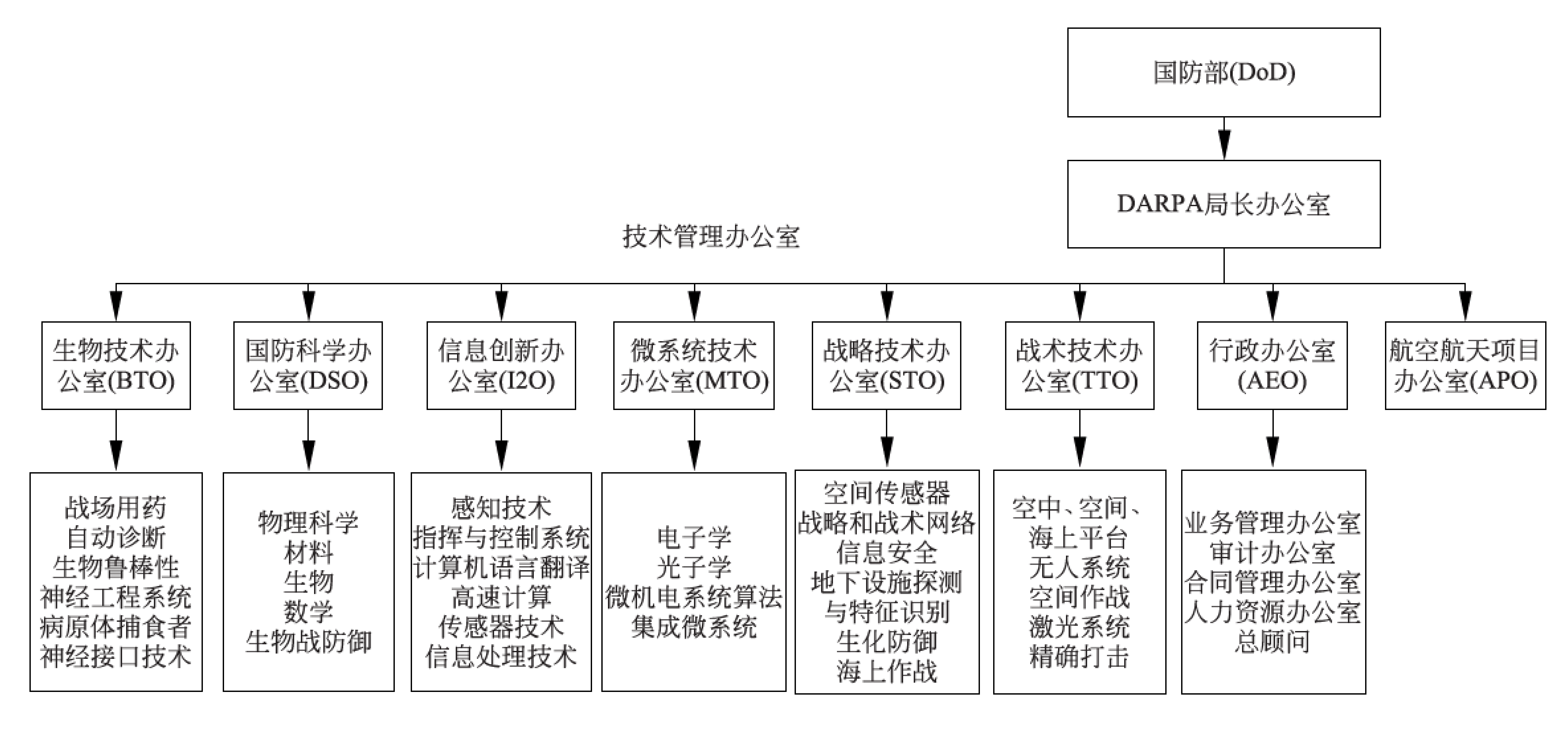


图 6-1　DARPA 组织架构

1. 战术技术办公室

战术技术办公室（Tactical Tcchnology Office，TTO）的主要职责是，为了占据对手无法实现的非对称新型军事技术优势，在最短时间内为军方创造前沿新型军事力量的技术研发办公室。TTO 的目标是在新型技术、武器和系统方面，

为军方提供高风险且具有高回报性的军事战略与战术。

2. 战略技术办公室

战略技术办公室(Strategic Technology Office, STO)主要负责将研发的新技术综合起来,上升到战略高度来推进军事作战能力。

3. 国防科学办公室

国防科学办公室(Defense Sciences Office,DSO)的主要任务是在国防科学技术的未知领域进行不断探索,提高国家国防安全技术水平。DSO 是基础科学和应用科学之间的一座桥梁,通过探寻和研究最有利于国防科学建设的创新想法,并通过理论研究与工程实践来将想法转化为可应用与军事领域的高端技术。

4. 信息创新办公室

信息创新办公室(Information Innovation Office,I2O)的主要职责是在影响战争规则的信息和软件科学技术领域来探索创新技术。这些信息和软件科学技术应用领域包括海洋、陆地、天空、太空等传统领域和网络空间及其他新兴领域。I2O 的主要研究内容包括,分析这些信息和软件技术应用领域的战争新模式,为美国及其盟友研发信息技术对抗武器。

5. 微系统技术办公室

微系统技术办公室(The Microsystems Technology Office,MTO)主要是在电子学、光子学、微机电系统算法和集成微系统等领域开展技术研发工作。

6. 行政办公室

行政办公室(The Adaptive Execution Office,AEO)的职责是在 DARPA 项目准备、启动、实施过程中,为 DARPA 的各部门做好行政服务工作。

6.2 网络空间项目 Plan X 介绍

6.2.1 Plan X 背景介绍

网络空间现在已被美国军方认为是一个关键性的战争领域,并且网络空间安全防护问题也已被上升为一个国家性安全问题。尤其是在关键基础设施安全

方面，致力于提升国家安全防护能力，DARPA 的信息创新办公室(I2O)在 2012 年 5 月宣布开展了一个名为 Plan X 的研究计划[1,2]，该计划是一个旨在为国防部研制一个集规划、实施和评价网络战功能的研究项目。Plan X 的主要目标是为普通的军队更好地提供网络操控工具和能力，因为军队现在恰恰急缺这样的网络空间能力。因此，DARPA 与 6 个公司签订了共计 7400 万美元的合同，研究如何在实时的、大规模的和动态的网络环境下正确地理解、规划和管理网络战争。

现代战争要求军队在军事行动中具备迅速计划、执行和评估的能力。国防部(DoD)在数十年的时间里对物理层面(陆地、海洋、天空和空间)进行了深入的研究。而网络空间，包括各种有线和无线连接、多种协议和设备、超级计算机以及嵌入式系统，已经成为一个新的作战领域。美国军方希望在网络空间领域中同样具备迅速计划、执行和评估各种军事行动的能力。

美国军方要通过 Plan X 来让军队清楚地认识到网络空间对军事的影响，对这个影响程度不仅要有一个精确的量化，而且还要清楚地认识到这些影响会带来的附带后果到底是什么。在网络战中，一方在网络空间中所采取的行动，当实施得当时，则可能毁掉敌方的网络，但是反之则又有可能会波及自己或同伴的网络。因此，Plan X 拟研究当我方实施网络行动后，如何避免产生波及自己的附带损害后果。目前美国军方在这方面也是非常欠缺。因此，如图 6-2 所示，为了更好地理解帮助美军理解和操控网络空间战争，Plan X 尝试借助美国虚拟现实科技公司 Oculus VR 的设备，帮助网络作战人员用一个三维立体的视角来分

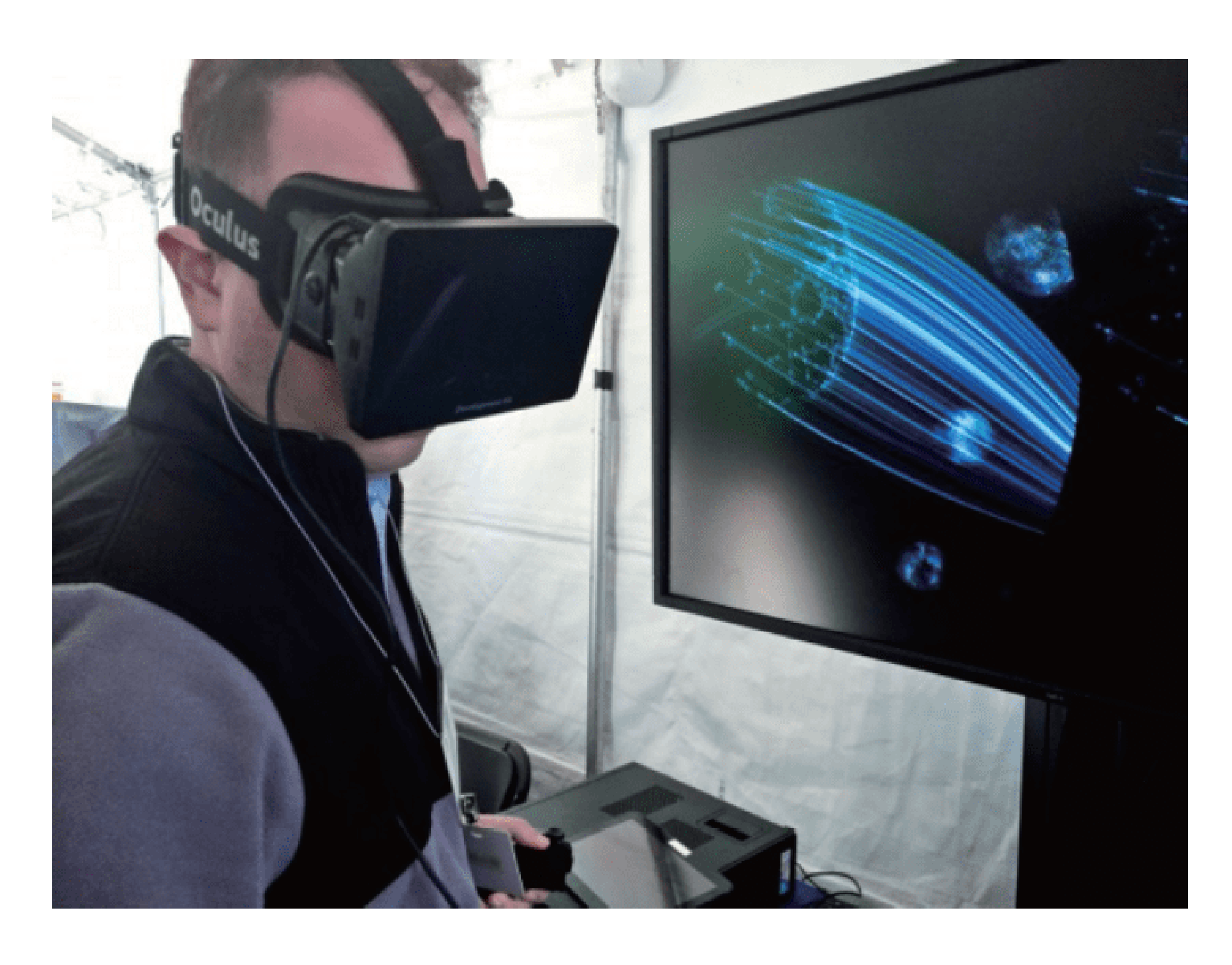


图 6-2 DARPA Plan X 项目负责研发人员展示 Oculus 网络战仿真

析、理解网络战[3]。Plan X 预计将在 2017 年完成,当然 Oculus VR 的软件或其他人机交互接口也有可能会在那之前完成。

6.2.2 Plan X 的特点

1. 军事人员全程参与

Plan X 拥有一支强大的工程师队伍,同时邀请作战人员作为最终用户持续参与,同工程师团队一起梳理工作流程,进行研制开发。

在军事人员与工程师团队的合作中,Plan X 旨在为军方提供一个统一的体系架构来实施网络作战行动,可视化显示网络空间态势,并对网络空间进行分析研究。

2. 网络边界防护

Plan X 关注的一个重要领域是,研究如何帮助作战人员在作战行动中确定对网络边界进行保护的流程。Plan X 提供的产品基于需要防护的网络关键部位,比如邮件和文件服务器、路由器和网关等,为作战人员制定网络作战计划,并对作战人员的操作、网络关键部位的运行状态进行可视化显示。Plan X 以可视化的方式显示网络的所有组成部分,作战人员能够清楚地看到它,就像用双筒望远镜看物理地形一样。

Plan X 计划是将军事科学应用于网络空间的计算机科学,为作战人员提供了一个他们能够理解网络战的平台。因为它是按照军事思维设计的,封装了军事决策的具体过程,允许作战人员像他们在新兵训练营和军事院校时训练时那样,制定作战计划,对网络空间进行研究分析。

3. 网络应用程序

实际上,作战人员往往并不具备这些网络工具所使用技术的“专业知识”,比如数字望远镜和传感器。为了解决这一难题,Plan X 的工程师们开发应用商店,并将众多工具转化为应用形式。

例如,Netstat 为网络防御人员所使用的典型应用之一,它能够帮助作战人员获取作战环境中的网络统计信息。这是一款独立的应用,掌握基础信息技术的用户都会使用。这正是此款特定工具的优势所在,其实际运行需要命令行参数进行操作。工程师团队对其中的复杂性进行抽象处理,从而确保网络计划人员能够以实际效果而不是孤立的术语进行合作与交流。

4. 发现数据模型

网络数据模型允许 Plan X 的工程师们严格定义网络空间中的术语和实体，例如，互联网协议地址、介质访问控制地址、网络接口或软件等。

在最初思考如何建立这套数据模型时，网络环境内存在大量事物需要以适当的方式加以界定。因此，他们着眼于现有数据模型并选定了 CybOX——即网络观测表达式[4]。

作为由联邦政府资助的研发中心，Mitre 公司利用 STIX 与 TAXII 标准进行模型开发。这项工作被纳入 2015 年的实施计划，旨在提升私营部门的网络安全信息共享能力。

5. 建立行动方案

行动方案是为应对潜在作战对手或突发情况而预先制定的作战计划。拟制行动方案，是为解决网络战部队缺乏明确的战斗计划和交战规则的问题，让网络战部队在一旦出现紧急情况时，能按照行动方案快速作出反应。

Plan X 项目组取得的另一个胜利是创建了计划构造模型，使得作战人员可以用可视化、图形化的方式建立网络作战行动方案。

6.2.3 Plan X 网络作战空间定义

因为军方以及供应商需要根据对网络空间的定义来进行建模分析，所以对网络作战空间进行清楚准备的定义是至关重要的。对网络作战空间的定义有三个主要概念，即网络图，运行单位、功能集[2]。

1. 网络图

对于一个给定的网络空间而言，有多种方式对其网络拓扑进行映射，包括路径追踪、数据包分析、静态架构图、动态路由协议更新等。网络图能够给出两个不同层面的网络空间信息：逻辑拓扑和元数据。

逻辑拓扑代表网络中计算机之间的直接联系，确定计算机数据包从源地址到目的地址的路由路径。逻辑拓扑包括被动的网络基础设施，如交换机、集线器和桥接，也包括主动网络覆盖的拓扑结构，如加密隧道、多协议标签交换和私密访问等。计算机网络的逻辑拓扑可以是静态或动态的。对网络空间的定义要求做到对当前逻辑拓扑状态的实时获取。高度动态的网络（如移动 Ad Hoc 网络），或共同控制消息协议遭到忽略或篡改的 IP 网络，都会给构建实时逻辑拓扑

带来较大挑战。

元数据,代表逻辑拓扑中每个元素的细节,包括链接能力、延迟和持久性。节点的元数据包括:链接的数量、操作系统补丁级别、协议、端口和其他信息。目前,元数据通常使用主动和被动扫描技术来获得,利用常见的计算机安全工具对其进行分析。

2. 运行单位

在逻辑拓扑确定后,可以将系统部署在运行单位。运行单位包括两个基本类型:输入节点和支撑平台。输入节点提供了对网络拓扑结构的直接物理访问接口(即输入节点是指一个操作员使用的计算机,可进行直接和协同操作)。

支撑平台部署一般有以下几种实现方式:①修改一台现有计算机,使其加入一个支撑平台;②修改现有的支撑平台;③通过扩展或修改现有的逻辑网络拓扑以对支撑平台进行实例化。

3. 功能集

网络作战空间中,功能集是指能够对网络战场进行影响与控制的应用技术集合。这些技术可以大致分为三个类别:访问权限,操作功能和通信技术。

访问权限允许设计师在电脑上执行任意指令,可以用来运行程序或有效载荷。对军事计划而言,这种技术一般用于计算机或支撑平台上,执行一个功能或通信技术来实现任务目标。操作功能代表所有其他类型的影响计算机和网络的技术,例如:rootkit、键盘记录、网络扫描仪、拒绝服务、网络/主机侦察、测量操作系统控制和影响。功能技术集越全面,军事计划者就越可以通过结合功能组件,制定更大规模的军事计划。

通信技术为输入节点及支撑平台提供了一系列用以交换信息和实现系统功能的通信方法。

6.2.4 Plan X 技术领域

为了建立 Plan X 的原型系统,DARPA 对系统架构、网络作战空间分析、任务部署、任务执行和直观界面五个技术领域进行了研究或资助。

1. 系统架构

系统架构团队建立 Plan X 系统基础设施,并支持整个系统的设计和开发。这些设计和开发工作包括设计安全架构、开发应用程序编程接口和制定数据格

式规范等。系统架构团队还负责采购系统硬件和维护整个基础设施系统。

系统架构团队主要关注以下两个重点：网络作战空间图形引擎的设计与实现，端到端的 Plan X 系统的设计与集成。

(1) 网络空间图形引擎

网络空间图形引擎是 Plan X 系统的核心。图形引擎的主要任务是对战场信息，以及其他 Plan X 系统组件进行接收、储存、检索和传输等操作。图形引擎从各种网络测绘组件和业务覆盖源等处接收实时的网络信息，并以此作为系统网络的整体信息，创建网络作战空间模型。Plan X 的所有其他组件将与此模型进行信息交互。网络测绘组件向图形引擎发送的数据能够帮助后者构建一个实时的逻辑拓扑。这些数据包括路由跟踪、链路延迟、边界网关协议（Border Gateway Protocol）、IP 生存时间、节点路由表信息及其他有助于构建逻辑拓扑的信息。

在逻辑网络拓扑中，业务覆盖信息被存储成每个元素的元数据。例如，业务覆盖信息包括操作系统标识、网络服务配置、防御和攻击能力和敌我识别信息等。此外，网络规划和运营信息也会有助于改进建立的网络作战空间模型。网络规划信息包括潜在的入口节点信息、平台部署位置信息、通信路径信息和通信接收者信息等。网络规划者可以查看对比网络部署与规划预定方案是否一致，并进行及时的分析和修改。网络运营信息包括网路入口状态信息、支撑平台运行状态信息、战斗损伤评估信息、战斗效果测量信息、战斗能力状态信息等。

基于上述网络测绘组件、业务覆盖源、网络规划和运营信息，Plan X 系统能够呈现出一幅全球网络作战空间的活动热力图，并给出作战行动计划和实际运行情况的对比图。这不仅将有助于网络作战规划人员对网络作战空间有一个全局视角的认识，并做出正确的网络作战部署，而且还能够帮助规划人员及时对网络布局做出调整。例如，当规划人员发现一个网络入口的流量已经快要达到瓶颈的时候，就可以及时启用另外一个网络入口。

(2) 端到端的 Plan X 系统

系统架构团队的另一工作重点是设计实现端到端的 Plan X 系统。这包括必要的人员设计与运营，研发 Plan X 系统和测试基础设施等工作。系统架构团队还对系统安全认证提供必要的管理，并与政府和其他技术领域的合作者合作，以确保系统能够支持所需的技术，满足军事规划和运作要求。

2. 网络作战空间分析

网络作战空间分析团队的主要任务就是建立网络作战空间分析模型，开发

自动化分析技术，帮助网络作战规划人员理解网络战场，制定战术可行的网络作战计划。此团队有两个研究重点：①通过开发自动化分析技术来协助军事规划者构建网络战计划；②提供演习支持，如模拟对手的进攻和防守，对演习整体规划进行优化。

（1）协助军事规划者构建网络战计划

网络作战空间分析团队需要对 Plan X 的信息进行分析和建模，这些信息包括但不限于节点选择、拓扑简化、支持平台布局、通信路径选择等信息。

① 节点选择

网络作战中的军事规划者在选择节点的时候需要网络作战空间分析团队提供协助。这些节点包括网络入口节点、目标通信节点、回避的节点等。网络作战空间分析团队可以帮助规划者根据其需要选择最佳的网络节点。

② 拓扑简化

当确定了网络入口节点集合和目标通信节点集合后，军事规划者需要从整个网络拓扑中选择一个最优的任务拓扑子集，即通过简化拓扑来实现最短路径、最小直径路由，或者使网络的最大延迟满足规划要求等目标。

③ 支持平台布局

当网络入口节点集合、目标通信节点集合和简化后的拓扑都确定了以后，军事规划者需要决定支持平台的最佳部署位置。

④ 通信路径选择

从网络入口节点到目标通信节点的众多通信路径中选择出最优路径的工作，如果是由人工来完成的话，显然是不切实际的。这就需要网络作战空间分析团队开发一种自动化路径选择技术。基于通信链路的连通性、最大网络延迟、回避节点和最大带宽等方面的要求，支持平台就可以完成通信路径的自动化选择工作。

（2）演习支持

网络作战空间分析团队的第二个研究重点是为网络战争演习提供技术支持。

3. 任务部署

任务部署团队的主要任务就是开发自动化任务部署技术。这种技术支持以一种图形化界面形式来构建任务计划脚本，并且还支持将多个不同的任务脚本自动地合成一个可执行的任务脚本。任务部署涉及的内容包括但不限于以下六方面。

(1) 运行检查点

任务部署过程允许规划者在任务执行过程中创建“检查点”，以此可以进行实时的运行操作信息监测和交互。规划过程可能还会要求网络运行者选择有顺序的行动，提供额外信息，或者提供行动路线。

(2) 实时的失效备援

任务部署过程应具有实时的失效备援功能，即当一个任务发生故障时，则另一个任务即可自动接手原失效任务所执行的工作。此外，失效备援还需要支持实时的人工操作控制功能，允许操作者能够直接彻底控制正在执行的任务。

(3) 自动操作水平

任务部署过程应该能够在网络通信链路中断或者恶化的情况下，仍能够确定如何实现自动化，以及确定在多大程度上实现自动化操作。规划者必须要标识出那些不需要人工干预就能够自动化执行的命令。

(4) 形式化分析

通过将任务计划转换成程序控制流图的形式，任务部署研究工作可以利用现有的程序分析和形式化分析方法。

(5) 实行交战规则

应该能够根据交战指挥官所制定的交战规则，通过编程和强制操作的方式来创建任务计划。在制定计划的时候直接引入交战规则，这样一来，任务部署过程就可以用形式化分析技术来验证操作人员对任务的消极影响和未授权行为。

(6) 网络战“剧本”

网络规划者可以事先研究制定一系列作战行动战术“剧本”，以此来辅助今后的作战规划和实际作战工作。这就类似于足球比赛中的战术安排，针对对手的不同情况，制定相应的应对战术。

4. 任务执行

任务执行团队将研发任务脚本运行环境和任务脚本执行的支撑平台。

任务脚本执行环境控制着整个任务的执行，支撑着实时操作交互过程，是实现 Plan X 计划的核心要素。任务脚本执行环境可以执行任务部署脚本，上传任务部署脚本到支撑平台，实施交战规则等功能。

在任务脚本执行的支撑平台中，任务执行团队则主要开发操作系统和虚拟机。高动态和敌对网络战任务在这些操作系统和虚拟机中运行。与军方有不同的交通工具(如坦克、无人机、轰炸机、战斗机、航空母舰等)执行不同的作战功能一样，军方也需要不同的网络战平台来执行不同的网络作战操作。这些支撑平

台包括但不限于以下四方面。

（1）“发射”平台（即主动进攻平台）

这些“发射”平台支持主动网络进攻能力部署、网络战前线部署、多个任务并发执行和网络入侵防御遏制等功能。

（2）网络战效果监测平台

网络战效果监测平台支持监测被攻和主动网络战任务执行效果、支持平台的运行状态、任务通信数据的完整性等功能。

（3）通信中继平台

在给定的网络拓扑中，通信中继平台可建立任务需要的特定网络路由路径，选定中继节点。通信中继平台可以满足多种类型通信协议、网络延迟和带宽要求。

（4）自适应防御平台

自适应防御平台支持网络防御功能，如过滤数据包和连接；将检测到的网络攻击信息通知其他支持平台；针对敌手攻击能力，采取相应的防御措施。

5. 直观界面

直观界面团队将设计 Plan X 的用户界面，包括工作流、直观的视图、动作研究和集成视觉应用。直观界面团队拟研发以下四种图形化界面来帮助用户与 Plan X 的各项功能进行人机交互。

（1）实时网络作战空间视图

实时网络作战空间视图的工作流图和视图关注的是大规模网络作战空间活动情况。该视图是所有正在进行的网络作战操作，部署计划和实时网络拓扑结构的热力图。该视图必须支持数据过滤功能，能够让网络作战指挥官快速地放大和查看正在进行的某个特定的网络战操作或部署计划。

（2）网络作战计划视图

网络作战计划视图是直观界面团队研发的四种图形化界面中最复杂的一种视图。直观界面团队应该在网络作战计划设计过程中，通过计划工作和概念性工作流图来描述作战计划。

（3）能力建设视图

整个网络作战计划过程应该完成特定网络作战能力的建设工作。这些能力将应用于今后实际的网络战中。因此，直观界面团队还应提供一种能力建设工作流图视图。

（4）网络战操控者控制视图

网络战操控者控制视图包括两类工作流图。第一类工作流图包括网络战操

作执行库和任务脚本的操作员接口。第二类工作流图在没有任务执行脚本的情况，为操控者提供一种实时的操控按键接口。

6.3　小结

DARPA 一直以来致力于开拓新的国防科研领域，研究分析具有潜在军事价值、风险大的新技术，验证新技术在军事上应用的可能性。随着网络空间安全防护问题，尤其关键基础设施安全被上升为一个国家性安全问题，DARPA 启动了名为 Plan X 的研究计划，旨在研发全面感知和理解网络空间作战的技术，并支持军事网络作战行动的可视化、任务规划和管理执行。本章重点介绍了 Plan X 对网络作战空间的定义、Plan X 涉及的技术领域和 Plan X 的特点。DARPA 凭借着在开拓新的科研领域和创新技术方面所做的工作，可以说是为美国的科技创新、军事创新立下了汗马功劳。DARPA 的成功，帮助美国在科技、军事等领域创立了不可动摇的领先地位。通过分析 Plan X 项目，可以发现美国在网络空间领域的奇思妙想确实值得我们深入学习和研究。

参考文献

[1] DARPA. Plan X. http://www.darpa.mil/program/plan-x

[2] DARPA. Broad Agency Announcement. Foundational Cyberwarfare (Plan X). DARPA-BAA-13-02. https://www.fbo.gov/utils/view? id=49be462164f948384d455587f00abf19

[3] Wired. DARPA turns Oculus into a weapon for cyberwar. https://www.wired.com/2014/05/darpa-is-using-oculus-rift-to-prep-for-cyberwar/

[4] Cybox. Cyber Observable eXpression(CybOX™). https://cyboxproject.github.io/

附录 A　名词及缩写词列表

AAA	Authentication, Authorization and Accounting	认证、授权和计费
AAL	Advanced Analytical Laboratory	先进分析实验室
AEO	Adaptive Execution Office	行政办公室
ANL	Argonne National Laboratory	阿贡国家实验室
ANT	Analyst Network Tool	分析师网络工具
APOD	Applications that Participate in their Own Defense	带有自我防御的应用
APT	Advanced Persistent Threat	高级持续性威胁
AQCESS	Accessible QKD for Cost-Effective Secret Sharing	量子密钥分发机制
ASD	Adaptive Self-Synchronized Dynamic Address Translation	自适应自同步动态地址转换
ASLR	Address Space Randomization or Address Space Layout Randomization	地址空间随机化或地址空间布局随机化
CART	Cyber Apex Review Team	网络顶点审查组
CAT	Crisis Action Team	危机行动小组
CDMA	Code Division Multiple Access	码分多址
CEIR	Correlating Extensive Incident Response	关联广泛事件响应
ChicagoFIRST	Chicago Fostering Industry Resilience and Security through Teamwork	芝加哥通过团队合作来培育工业安全性与弹性
CI	Critical Infrastructure	关键基础设施
CIKR	Critical Infrastructure and Key Resource	关键基础设施核心资源

CMT	Consequence Modeling Tool	结果建模工具
COOP	Continuity of Operations	继续运作
CPS PWG	Cyber-Physical Systems Public Working Group	CPS公开工作组
CRISP	Critical Resilient Interdependent Infrastructure Systems and Processes	重要基础设施和过程的弹性相互依赖
CS	Cyber Storm	网络风暴
CSCSWG	Cross Sector Cyber Security Working Group	跨部门网络安全工作组
CSD	Cyber Security Division	网络安全局
CSET	Cyber Security Evaluation Tool	网络安全评估工具
CTIIC	Cyber Threat Intelligence Integration Center	网络威胁情报整合中心
CVSS	Common Vulnerability Scoring System	普遍脆弱性评分系统
D2D	Device-to-Device	设备到设备
DAR	Design Architecture Review	设计架构评审
DARPA	Defense Advanced Research Projects Agency	美国国防部先进研究项目局
DATES	Detection and Analysis of Threats to the Energy Sector	能源行业的威胁检测和分析
DDoS	Distributed Denial of Service	分布式拒绝服务
DETER	DEfense Technology Experimental Research	防御技术实验研究
DETERLab	DEfense Technology Experimental Research Laboratory	防御技术实验研究实验室
DHS	Department of Homeland Security	国土安全部
DMZ	Demilitarized Zone	隔离区
DNP3	Distributed Network Protocol Version 3	分布式网络协议第三版本

DoD	Department of Defense	国防部
DoE	Department of Energy	能源部
DoE-OE	Department of Energy's Office of Electricity delivery & energy reliability	电力调度与能源可靠性办公室
DoS	Denial of Service	拒绝服务
DSO	Defense Sciences Office	国防科学办公室
DyNAT	Dynamic Network Address Translation	动态网络地址转换
EAGLE	Environment for Analysis of Geo-Located Energy Information	基于地理的能源信息分析环境
EIOC	Electricity Infrastructure Operations Center	电力基础设施运营中心
EMIST	Evaluation Methods for Internet Security Technology	互联网安全技术评估方法
EO	Executive Order	行政令
ESF	Emergency Support Function	应急支持功能
FETS	Government Emergency Telecommunications	政府紧急电信服务
FPGI	Future Power Grid Initiative	未来电网倡议
GAME	Graphical Adversary Modeling Environment	图形化对手建模工具
GCC	Government Coordination Committee	政府协调委员会
GISLA	Government Information Security Leadership Awards	政府信息安全领导奖
GSM	Global System for Mobile Communication	全球移动通信系统
HAS	Homeland Security Act	国土安全法
HMI	Human Machine Interface	人机接口
HPS	Host Protection Strategies	主机保护策略
HSARPA	Homeland Security Advanced Research Projects Agency	国土安全部高级研究计划局

HSIN	Homeland Security Information Network	国土安全信息网络
HSOC	Homeland Security Operation Center	国土安全运营中心
HVAC	High Voltage Alternating Current	高压交流电
HVDC	High Voltage Direct Current	高压直流电
I2O	Information Innovation Office	信息创新办公室
ICCP	Inter-Control Center Communications Protocol	内部控制中心通信协议
ICI	Interdependent Critical Infrastructure	相互依赖的关键基础设施
ICSJWG	Industrial Control System Joint Working Group	工业控制系统联合工作组
IDS	Intrusion Detection System	入侵检测系统
IEC	International Electrotechnical Commission	国际电工委员会
IIMG	Interagency Incident Management Group	跨部门事件管理小组
INL	Idaho National Laboratory	爱达荷国家实验室
IPS	Intrusion Prevention Systems	入侵防御系统
ISA	International Federation of the National Standardizing Associations	国际标准化协会
ISAC	Information Sharing and Analysis Center	信息共享和分析中心
ISAO	Information Sharing and Analysis Organizations	信息共享和分析组织
ISR	Instruction Set Randomization	指令集随机化
IWWN	International Watch and Warning Network	国际观察和预警网络
LANL	Los Alamos National Laboratory	洛斯阿拉莫斯国家实验室

LOGIIC	Linking the Oil and Gas Industry to Improve Cyber Security	将石油和天然气工业连接起来增强网络安全
MS-ISAC	Multi-State Information Sharing & Analysis Center	多州联合的信息共享与分析中心
MT6D	Moving Target IPv6 Defense	基于 IPv6 的移动目标防御
MTD	Moving Target Defense	移动目标防御
MTO	Microsystems Technology Office	微系统技术办公室
MUTE	Mutable Networks	突变网络
NASR	Network Address Space Randomization	网络地址空间随机化
NCCIC	National Cybersecurity and Communications Integration Center	国家网络安全与通信集成中心
NCRCG	National Cyber Response Coordination Group	国家网络响应协调小组
NCSD	National Cyber Security Division	国家网络安全局
NERC	Natural Environment Research Council	自然环境研究委员会
NGCI	Next Generation Cyber Infrastructure	下一代网络基础设施
NHERI	Natural Hazards Engineering Research Infrastructure	自然灾害工程基础设施研究
NIPP	National Infrastructure Protection Plan	国家基础设施保护计划
NIST	National Institute of Standards and Technology	国家标准与技术研究院
NPPD	National Protection and Programs Directorate	国家保卫与计划指挥部
NSA	National Security Agency	国家安全局

NSF	National Science Foundation	国家科学基金会
NSIEs	Network Security Information Exchanges	网络安全信息交流
NSTB	National SCADA Test Bed	国家 SCADA 测试床
OF-RHM	OpenFlow Random Host Mutation	开放流随机主机突变
ORNL	Oak Ridge National Laboratory	橡树岭国家实验室
PCII	Protected Critical Infrastructure Information	保护关键基础设施信息
PCIS	Partnership for Critical Infrastructure Security	关键基础设施安全伙伴关系
PCS	Process Control System	过程控制系统
PDD	Presidential Decision Directives	总统令
PLC	Programmable Logic Controller	可编程逻辑控制器
PNNL	Pacific Northwest National Laboratory	西北太平洋国家实验室
PowerNET	Power Networking Equipment and Technology	电网网络设备和技术
RHM	Random Host Mutation	随机主机突变
RIRN	Remote Incident Response Network	远程事件响应网络
RRAP	Regional Resiliency Assessment Program	区域弹性评估程序
RTDS	Real Time Digital Simulator	实时数字仿真器
RTU	Remote Terminal Unit	远程终端单元
SAV	Sender Address Verification	源地址验证
SCADA	Supervisory Control And Data Acquisition	数据采集与监视控制
SCC	Sector Coordinating Committee	行业协调委员会
SCIT	Self Cleansing Intrusion Tolerance	自清洗入侵容忍技术
SG-CG	Smart Grid Coordination Group	智能电网协调小组

SGIP	Smart Grid Interoperability Panel	智能电网的互操作性小组
SIS	Safety Instrumented Systems	安全仪表系统
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council	州、地方政府、部落协调委员会
SNL	Sandia National Laboratory	桑迪亚国家实验室
SOP	Standard Operating Procedure	标准操作流程
SSCP	Secure SCADA Communications Protocol	安全 SCADA 通信协议
STD	Science and Technology Division	科学与技术局
STO	Strategic Technology Office	战略技术办公室
TCIPG	Trustworthy Cyber Infrastructure for the Power Grid	使得智能电网中的网络基础设施变得可信
TTO	Tactical Technology Office	战术技术办公室
TWWG	Trustworthy Wireless Working Group	可信赖无线工作组
UCG	Unified Coordination Group	统一协调小组
UCSD	University of California, San Diego	加州大学圣迭戈分校
UMTS	Universal Mobile Telecommunications System	通用移动通信系统
USC ISI	University of Southern California, Information Sciences Institute	南加州大学信息科学研究所
US-CERT	United States Computer Emergency Readiness Team	美国计算机应急预备小组
USSS	United States Secret Service	美国特工处
VCSE	Virtual Control System Environment	虚拟控制系统环境
WiMAX	Worldwide Interoperability for Microwave Access	全球微波互联接入
WPS	Wireless Priority Service	无线优先级服务

附录 B　美国关键基础设施安全之物联网安全调研

随着工业信息化和自动化的不断发展与变革，工业物联网作为工业系统自动化与传感技术和云计算大数据等技术高度融合的产物，可通过工业设备之间、设备与人之间的互联互通，云计算和大数据分析，充分发挥设备与系统的潜能，深度优化产业结构，极大地提高工业生产产能和效率。

工业控制系统或工业物联网作为国家基础设施的重要组成部分，支撑着能源、通信、金融、交通、公用事业等重要行业的正常运转。因此，本附录将单独介绍美国在物联网安全方面所指定的一些战略或建议报告。

B.1　美国国土安全部保障物联网安全战略原则报告简介

美国国土安全部于 2016 年 12 月 15 日发布了一份《保障物联网安全战略原则报告》。该报告阐述了物联网安全总体原则，确定了在政府和行业工作中需要加强的物联网安全防护重点。

B.1.1　介绍和概览

物联网（IoT）的网络连接设备，系统和服务的增长为我们的社会创造了巨大的机会和利益。而物联网自身安全却跟不上创新和部署的快速步伐，造成了重大的安全和经济风险。本文档解释了这些风险，并提供了一套非约束原则和最佳实践的建议，来为设备和系统业务设计、制造、使用和运营构建一个负责任的安全级别[1]。

（1）物联网的增长和流行

互联网连接的设备实现了人、网络和物理设施之间的无缝连接。这些连接具有高的效率、新颖用途和定制体验，吸引着制造商和消费者。网络连接的设备已经在日常生活的许多方面变得无所不在，甚至是必不可少的，从健身跟踪器、起搏器和汽车到向我们的家庭提供水和电力的控制系统，物联网提供的服务几乎没有限制。

（2）确定物联网安全优先级

虽然物联网的好处是不可否认的，但现实是，安全性跟不上创新的步伐。随着人们越来越多地将网络连接集成到国家的关键基础设施中，原来人工完成的重要过程（并因此拥有免疫措施来抵抗恶意网络活动）现在很容易受到网络威胁。越来越多的国家对网络连接技术的依赖比保护它的手段增长得更快。

物联网生态系统引入了风险，包括恶意行为操纵网络设备来回的信息流动或篡改设备本身，这些导致敏感数据的盗失和消费者隐私的丢失、业务操作的中断、大规模分布式拒绝服务攻击带来的互联网减速，以及关键基础设施潜在的毁坏。

2015年，从网络攻击导致乌克兰部分地区电网暂时停电事件中，世界看到了连接系统的故障可导致严重的后果。因为我们国家现在依赖正常运作的网络来维护如此多的生命需要的基础设施，物联网安全现在已经成为国土安全的问题。

政府和行业必须尽快合作，确保物联网生态系统建立在可信赖和安全的基础之上。2014年，总统国家安全电信咨询委员会（NSTAC）强调需要采取紧急行动。

物联网的应用不断在速度和范围上增加，并将几乎影响我们社会的所有部门。确保物联网的应用不会带来不应有的风险是国家面临的重要挑战。此外，有一个很小且快速闭合的窗口期，来保证物联网以最大化安全最小化风险的方式应用。如果国家没能成功把握机会，它将会对几代人带来安全影响。

现在是解决物联网安全的时候了。本文件为公共和私营部门参与这些关键问题设置了阶段。第一步是在物联网开发者、制造商、服务提供商以及购买和部署这些设备、服务和系统的用户之间，激励和构建关于物联网安全积极措施的对话。以下原则和实施建议提供的策略集中在IOT安全方面，增强了加固IOT微系统的可信架构。

（3）战略原则概述

通过公认的最佳安全做法能够减少物联网的许多安全缺陷，但今天太多产品没有实现基本的安全措施。有很多成因导致这种安全缺陷，一是不清楚谁应该为安全责任负责，一家公司设计设备，另一家公司提供组件软件，再一家公司操作嵌入设备的网络，以及还有一家公司部署这些设备。由于缺乏综合的、广泛采用的物联网安全国际规范和标准，这一挑战更加突出。其他成因还包括缺乏激励开发者研发安全产品，因为他们不一定承担这样做的成本，甚至没有意识到如何评估竞争选项的安全特征。

需要为利益相关者提供一种关于他们如何解决些物联网安全挑战的思考的方法：

① 在设计阶段结合安全；

② 启用安全更新和漏洞管理；

③ 建立在可靠的安全实践之上；

④ 根据潜在影响确定安全措施的优先级；

⑤ 提升物联网的透明度；

⑥ 连接需仔细谨慎。

随着物联网安全工作的不断努力，政府和私营企业共享责任，物联网风险将持续地减缓。公司和消费者通常对他们制造或购买产品的安全特征做出的自己决定负责。在某些特定监管环境和执法活动之外，政府的作用是提供工具和资源，以便公司、消费者和其他利益相关者能够就物联网安全做出明智的决策。

（4）范围、目的和受众

这些非约束性原则的目的是为利益相关者提供在开发、制造、实施或使用网络连接设备时帮助解决安全问题的建议做法。具体来说，这些原则的目的是：

① 物联网开发人员，在设计和开发设备、传感器、服务或物联网的任何组件时应考虑安全问题；

② 物联网制造商，应提高消费者设备和供应商管理设备的安全性；

③ 服务提供商，通过物联网设备实现服务，考虑这些物联网设备提供的功能安全性，以及支持这些服务的基础设施的安全性；

④ 工业和商业级消费者（包括联邦政府和关键基础设施所有者和运营商），应作为领导者参与制造商和服务提供商提供安全物联网设备。

B.1.2　战略安全保障原则

以下阐述的原则旨在提高物联网在设计、制造和部署阶段的安全性。广泛采用这些战略原则和相关建议的做法将大大提高物联网的安全态势。然而，没有一种适合所有情况的解决方案来减轻物联网安全风险。以下列出的所有实践在物联网设备的多样性中将同样重要。这些原则旨在考虑相关业务环境以及涉及网络连接的设备，系统或服务的事故可能导致的特定威胁和后果的方式进行调整和应用。

（1）在设计阶段结合安全

安全性应被评估为任何网络连接设备的必要部分。虽然有例外，但在许多情况下，经济驱动力或对风险意识的缺乏使得企业将设备推入市场时很少考虑

安全。在设计阶段结合安全,可以避免产品在开发和部署之后因安全问题带来的潜在业务中断和高昂重建成本。通过注重网络设备安全性,也能为生产商和服务商提供市场分化机遇。以下做法是在设计、开发和生产的最早阶段解决安全问题的一些最有效的方法。

建议操作:默认情况下安全性是通过唯一的、难以破解的缺省用户名和密码来保障。用户通常不会修改由生产商提供的物联网设备的缺省用户名和密码,导致其用户名和密码很容易被破解。僵尸网络通过不断扫描使用生产商提供的默认用户和密码的物联网设备来运行。强壮的安全控制应该是让用户具有修改禁用某些功能的权限。

使用技术和经济可行的最新操作系统构建设备。许多物联网设备使用Linux操作系统,但没有使用最新的操作系统。使用最新操作系统确保已知漏洞都被修补。

使用硬件集成安全特性增强设备的保护和完整性。例如,在处理器中嵌入晶体管级的安全集成芯片,并提供加密和匿名功能。

在设计中考虑系统和操作中断。了解设备故障可能导致的后果将使开发人员、制造商和服务提供商做出更明智的基于风险的安全策略。在可行的情况下,开发人员应构建物联网设备考虑其失效可能带来的安全后果,从而防止失效导致更大的系统中断。

(2) 推进安全更新和漏洞管理

即使在设计阶段考虑了安全性,但在产品部署后发现漏洞也很常见。这些漏洞能通过补丁、安全更新和漏洞管理策略缓解。在设计这些策略时,开发人员应考虑设备故障的影响、相关产品的持久性以及预期的维修成本。在没有部署安全更新能力的情况下,制造商可能面临昂贵的召回成本并召回具有已知的漏洞的设备。

建议操作:考虑通过网络或其他自动化方式对设备进行安全保护。理想情况下,自动对程序打修补丁,并利用加密完整性和认证保护来更快地修补漏洞。

考虑协调第三方供应商来进行软件更新,以修补漏洞和改进安全性,确保消费者设备具有一整套的安全防护措施。

开发解决漏洞的自动化机制。例如,在软件工程领域存在从实时的研究和黑客团体的关键漏洞报告中提取信息的机制。这允许开发人员在软件设计阶段修补这些漏洞,并适时做出响应。

制定关于协调漏洞的披露政策,包括相关的安全措施以解决已知的漏洞。协调披露政策应包括开发人员、制造商和服务提供商,并包括提交给计算机安全

事故响应小组(CSIRT)的有关任何漏洞的报告信息。美国计算机应急相应小组(US-CERT)、工业控制系统(ICS)-CERT 和其他 CSIRT 提供定期技术警报,包括在重大事件后提供关于漏洞修补和缓解的措施。

制定物联网设备的使用期限策略。并不是所有的物联网设备都会无限期地修补和更新。开发人员应该提前考虑产品使用期限问题,并告知制造商和消费者在超出设备使用期限后,使用设备可能存在的风险。

(3) 建立在可靠的安全实践之上

许多验证过的传统 IT 和网络安全实践可以应用于 IoT 领域。这些方法可以帮助发现漏洞,检测合规性,响应潜在事件,并从 IOT 设备的损坏或中断中恢复。

国家标准与技术研究所(NIST)发布了一个网络安全风险管理框架[2],该框架已被私营企业、部门和组织内部广泛采用。该框架被广泛认可为组织网络风险管理的一个全面的试金石。尽管不是针对物联网,但风险框架为考虑风险和最佳实践提供了起点。

建议操作:从基本的软件安全和网络安全实践开始,并以灵活、适配和创新的方式应用于 IoT 生态系统。

参考相关部门的具体指导,作为考虑安全实践的起点。一些联邦机构针对其管理的特定部门制定了安全实践。例如,国家公路交通安全管理局(NHTSA)最近发布了关于现代车辆网络安全最佳实践的指南,解决了自动或半自动车辆带来的一些特殊风险。同样,食品和药物管理局发布了医疗器械网络安全市场管理指南草案。

执行深度防御。开发人员和制造商应该采用整体的安全策略,包括针对网络安全威胁的分层防御机制,以及用户级工具作为恶意角色的潜在入口点。如果修补或更新机制不可用或不足以修补漏洞,深度防御措施将特别有价值。

参与信息共享平台,实时报告并接收漏洞,收到公共和私人合作伙伴中获取的当前网络威胁和漏洞的重要信息。信息共享是确保利益相关者在出现威胁时了解威胁的关键。国土安全部(Department of Homeland Security, DHS)国家网络安全和通信集成中心(National Cybersecurity and Communications Integration Center, NCCIC),以及不同国家及其部门的信息共享和分析中心(Information Technology-Information Sharing and Analysis Center, ISAC)和信息共享和分析组织(Information Sharing and Analysis Organizations, ISAO)。

(4) 根据潜在影响优先考虑安全措施

风险模型在物联网生态系统中存在显著差异。例如,工业消费者(例如核反应堆所有者和操作者)与零售消费者有不同的考虑。不同客户安全失效带来的

后果也有很大差异。因此，专注破坏、泄露或恶意活动的潜在后果对决定物联网生态系统的安全方向以及最好的减缓重大后果至关重要。

建议操作：在可能的情况下了解设备的预期用途和环境。这种意识能够帮助开发人员和制造商考虑 IoT 设备的技术特性、设备如何操作以及可能需要的安全措施。

执行“红队”练习，开发人员主动尝试绕过应用程序、网络、数据或物理层所需的安全措施。由此产生的分析和安全增强计划应有助于优先决定在何处和如何采用额外安全措施。

识别和验证连接到网络的设备，尤其是工业用户和商业网络。对已知设备和服务应用认证措施，允许工业消费者控制其组织框架内的那些设备和服务。

（5）提升物联网的透明度

在可能情况下，开发人员和制造商需要了解供应链，了解组织外供应商提供的软、硬件部件是否有任何的相关漏洞。依赖于许多低成本、易于获取的应用在物联网中软硬件解决方案，了解相关信息可能会成为挑战。由于开发人员和制造商依赖外部资源提供低成本、易于获取的软硬件解决方案，因此在开发和部署物联网设备时，他们可能无法准确评估组件中内置的安全级别。此外，由于许多物联网设备利用开源包，开发人员和制造商可能无法确定这些组件部分的来源。

增强意识可以帮助制造商和工业消费者识别安全措施应用的位置和具体方法，或者冗余建设。根据相关产品的风险状况，开发人员、制造商和服务提供商将更有能力尽快适当地缓解威胁和漏洞，无论是通过修补、产品召回还是消费者咨询。

建议操作：

在可能的情况下，考虑内部和第三方供应商进行端到端风险评估。开发商、制造商和供应商应参与风险评估过程，使他们能够意识到潜在的第三方脆弱性，并促进信任和透明。安全性应该随着供应链中组件更换、删除或升级而重新评估。

考虑创建一个关于漏洞报告的公开披露的机制。例如，Bug Bounty 计划依靠众包方法来识别公司内部安全团队可能没有捕获的漏洞。

考虑开发和使用软件材料的清单，用作构建供应商和生产商之间的共享信任机制。开发人员和制造商应考虑在设备包中提供已知硬件和软件组件的列表，通过该方法满足保护知识产权的需要。列表可以作为物联网生态系统中其他人有价值的工具，以了解和管理其风险，并在发生任何事件后立即修复任何漏洞。

（6）小心谨慎接入

考虑物联网的使用和物联网被破坏的相关风险，物联网消费者，尤其是工业企业应该小心并谨慎考虑是否持续联网。物联网消费者还可以通过小心谨慎地接入来衡量网络连接带来的潜在威胁，以及衡量物联网设备潜在的破坏或故障的风险，以及限制连接到互联网上的成本。

在当前联网环境中，任何给定物联网设备可能在其生命周期期间被中断。物联网开发人员、制造商和消费者应考虑中断会如何影响物联网设备的主要功能和业务操作。

建议操作：

向物联网用户提供任何网络连接的预期用途。可能不需要直接互联网连接来操作物联网设备的关键功能，特别是在工业环境中。关于连接的性质和目的的信息可以告知消费者来决定。

进行有意地连接。有些情况下，消费者不想直接连接到互联网，而是连接到可以聚合和评估任何关键信息的本地网络。例如，工业控制系统（ICS）应通过 ICS-CERT 发布的推荐原则[3]来进行保护。

内置控件，允许制造商、服务提供商和消费者在需要或希望时禁用网络连接或特定端口，以启用选择性连接。根据物联网设备的用途，向消费者提供对终端实施的指导和控制是一种良好的做法。

B.1.3　结论

我们的国家无法承担一代未考虑安全的部署的物联网设备。考虑到关键基础设施，个人隐私和经济的潜在危害，代价太高，后果不堪重负。

由于 DHS 发布这些原则，认识到我们在其他联邦机构的同事正在努力，推进架构和建立实践来解决物联网的安全问题。本文件是通过阐明总体安全原则加强这些努力的第一步。但是，肯定需要下一步。

DHS 确定了应该在政府和行业中加强物联网安全的四个方面的努力。

（1）协调各个联邦部门和机构与物联网利益相关者进行互动合作，共同探索新方法来减轻物联网带来的风险

DHS 与其联邦合作伙伴将继续与行业合作伙伴进行合作，以确定可进一步加强 IoT 安全性的方法，并促进对可能解决 IoT 风险的不断发展的技术趋势的理解。今后的努力还将侧重于更新和应用这些原则，进一步完善和理解这些方法。

（2）建立利益相关者的物联网风险意识

重要的是，利益相关者应了解物联网风险，以便他们能够定位自己如何解决

这些风险。DHS 将与其他机构、营部门和国际合作伙伴合作，增强公众意识、教育和培训计划。DHS 与其他机构一起，还将对特定部门和个人消费者采取更直接的举措。

(3) 识别并推进纳入物联网安全的激励措施

政策制定者、立法者和利益相关者需要考虑如何更好地激励增强物联网安全性的努力。在当前环境中，常常不清楚谁对某一产品或系统的安全负有责任。此外，安全性差所带来的成本通常不由增强安全的人承担。DHS 和所有其他利益相关方需要考虑侵权责任、网络保险、立法、监管、自愿认证管理、标准设定举措、自愿行业级计划和其他机制来改善安全，同时仍然鼓励经济活动和突破性创新。今后，DHS 将召集合作伙伴谈论这些重大事项，并收集意见和反馈。

(4) 致力于物联网的国际标准开发过程

IoT 是全球生态系统的一部分，美国与其他国家和国际组织正在全力应对同样的安全问题，开始评估众多同样的安全考虑。重要的是，IoT 相关活动不会分裂成不一致的标准或规则集。随着 DHS 越来越注重物联网的努力，我们必须与国际合作伙伴和私营部门合作，支持国际标准的发展，并确保它们符合我们对促进创新和促进安全的承诺。

DHS 期待着这些下一步的合作步骤。合作将确保网络连接的未来不仅是创新，而且安全和建设更为持久。

B.2 美国国家安全电信委员会物联网报告简介

美国国家安全电信委员会于 2014 年 11 月 19 日发布了一份《物联网报告》。该报告介绍了物联网概论，分析了物联网在国家安全和应急准备工作中发挥的作用，探讨了物联网给人类社会带来的影响。

B.2.1 报告综述

智能、自适应、连通的物联网设备正在快速普及，应用在几乎所有的关键基础设施部门中，且其发展速度远远超过此前的技术。物联网将显著提高社会发展的效率，其中许多物联网技术已经被实现，彻底地提高了社会效率，诸如系统故障的早期发现、可靠性和应变能力的提高等。但是物联网设备的快速普及和连接也带来了许多风险，包括新的攻击方式、新的漏洞等。也许我们最关心的是，使用远程访问造成物理设备破坏的可能性越来越大[4]。

意识到这一点，美国总统行政办公室，特别是国家安全委员会，在国家安全

和应急准备(National Security and Emergency Preparedness，NS/EP)的背景下，任命国家安全电信咨询委员会(National Security Telecommunications Advisory Committeen，NSTAC)研究物联网中的网络安全含义。NSTAC 发现物联网的应用速度不断加快、覆盖范围也将越来越广，最终将影响人类社会的方方面面。国家面临的挑战是确保物联网的应用不会产生不必要的风险，此外，NSTAC 还认为，在物联网系统中必须有一个“较小的、能快速关闭的窗口”确保物联网风险最小化，如果国家不这样做，物联网的风险将一直影响到后代。

2014 年 2 月，NSTAC 发布了工业互联网的研究报告，总结了 NSTAC 工业互联网研究下属机构的工作。该报告显示，除了工业互联网，物联网还被称为其他几个术语，包括：机器到机器通信、万物的互联网、网络化的物理系统。在报告中，NSTAC 将物联网描述为全球基础设施的扩展，其主要通过现有的和不断发展的信息技术，结合物理系统和虚拟网络系统的连接，实现新的自动化能力。该报告还指出，物联网的潜在好处包括能推动创新服务的发展，在许多情况下，这促使我们能更有效地利用基础设施。然而，研究发现政府和企业必须考虑物联网的几个安全因素，包括攻击范围迅速扩大、千变万化的威胁环境、隐私问题、动态集中的网络攻击、硬件生命周期的改变等。NSTAC 认为物联网的这些利益和风险在早期部署的时候已经被大家公认了，因此，更好地了解这种技术、现有的和新的政策结构的含义以及它对关键基础设施安全性和稳定性的影响非常重要。为深化对这种技术的研究，在 NS/EP 的背景下，NSTAC 建立了物联网(IoT)研究小组去研究物联网中网络安全的影响。

在 2008，美国国家情报委员会预测“到 2025 年，物联网将是一个颠覆性的技术”。该委员会同时强调，个人、企业和政府都没有做好准备去迎接一个网络接口驻留在日常用品各个方面的未来。近六年后，这一预测仍然是有效的，但现在看来，物联网将被破坏却远远早于 2025 年。国家情报局(DNI)表示“这些系统的复杂性和本身性质意味着安全没有保障，不法分子可能会很轻松地对这些系统造成安全问题 ”。一些统计数据验证了政府的担忧：在 2008 年互联网连接设备的数量第一次超过人口数量，而且这个数字还在继续增长，增长速度比人口增长数量更快。到 2013 年，有多达 130 亿个设备接入互联网，并且预测表明，到 2020 年，这个数量将增长到 500 亿或更多，这些设备在全球将产生超过 8 兆美元的收入。其中，许多系统对任何用户，包括恶意攻击者都是可见的，因为搜索引擎已经爬取了整个互联网的索引，识别出了连接的设备。

物联网是近几十年来在通信、网络、处理能力、小型化和应用创新方面上的最新发展，并从根本上改变了通信、网络和传感器。物联网是由一些离散的对

象、应用程序和在物理世界中可以感知、记录、解释、通信、处理各种信息或控制设备的服务组成的网络。然而,物联网不同于以前技术的发展情况,因为它超越了计算机网络的限制,并直接连接到物理世界。正如现代通信已经从根本上改变 NS/EP,物联网也有类似的革命性的影响。

纵观整个通信革命,大量现有的和新的技术使得生产效率显著提高,并且政府和私营部门业务和效益能力也得到惊人的改善。同时,物联网在联网设备的部署速度、规模和广度方面各不相同,也使得个人和组织都获得了巨大效益。尽管物联网带来的好处是非常明显的,但同时也伴随着一些风险。增加的依赖关系、数量不断增长的设备以及设备的互联都将产生一个巨大的攻击面和众多的潜在威胁。扩大的攻击面和国家对这些新系统的依赖,无论是直接或间接嵌入到关键基础设施系统,都将使物联网和新系统成为犯罪分子、恐怖分子、图谋不轨的国家的目标。这些依赖关系将不断增加,物联网将渗透到经济的各个部门和人民生活的各个方面。然而所有的用户都必须应付这种扩大的攻击面,物联网在国家安全领域的应用都必须针对潜在的风险进行强化。随着 IoT 制造商和供应商努力满足客户的需求,包括 NS/EP 需求,竞争将最终决定哪些产品和服务成功或失败,从而推动进一步的创新。

认识到物联网发展的速度、应用的广度、部署的深度,总统行政办公室,特别是国家安全委员会,要求国家安全电信咨询委员会(NSTAC)在 NS/EP 背景下进行物联网网络安全的研究。2013 年 10 月,NSTAC 指定的联邦官员建立了工业互联网范围的小组研究这个问题,并为 NSTAC 提供相关信息。经过批准后,研究小组于 2014 年 3 月正式成立。报告[4]主要探讨物联网爆炸性增长对 NS/EP 领域的影响,并将重点介绍对 NS/EP 敏感基础设施的安全状态和相关战略产生的潜在变化。报告主要考虑以下几个方面:潜在网络攻击面的巨大扩展和变形,物联网引发的数据爆炸的影响,以及开发关注物联网、信息技术、运营技术的新学科的需要。

新兴的物联网技术被部署在从个人到国家系统的不同范围,NSTAC 采取的方法是以此为指导的。为了获得与物联网技术实施相关的关键概念、最佳实践和经验教训,NSTAC 与一些联邦政府组织和行业专家进行洽谈,与业界的几个行业领先的组织进行合作,这些组织致力于帮助塑造未来最好的物联网。此外,在 NSTAC 工业互联网范围界定报告中,确定了物联网的四个研究领域,以帮助形成 NSTAC 的如下四点研究工作:

(1) 安全:诚信、弹性、用户行为、公共/私人合作伙伴关系;

(2) 操作:系统的互操作性,操作的可靠性,频谱优先级,IT/OT 过程协调;

（3）设计：最佳实践和标准，按设计安全，信任关系，与 NS/EP 方案的集成；

（4）政策：弹性、隐私、公共安全、国际因素。

此外，NSTAC 还进行了 SWOT 分析（优势、劣势、机会、威胁），针对 NS/EP 背景下进行 SWOT 分析，强调了物联网的效益和风险，这一分析有助于 NSTAC 考虑物联网技术建议的优先级。

B.2.2　物联网概论

物联网系统支撑着美国社会的每一个方面，从交通到公共事业到通信，系统可以接受来自全世界的访问和控制。越来越多的设备连接到网络，这些网络彼此相连，这就是物联网。但是，没有统一定义的物联网，没有一个统一的协议确定使用该名称来描述这种趋势。无论是所谓的物联网、工业网络或网络物理系统（CPS），这些术语描述的物联网都是由一些离散的对象（或设备）、应用程序和在物理世界中可以感知、记录、解释、沟通、处理各种信息并采取行动或控制设备的服务组成的网络。这些设备的覆盖范围从普通消费者设备上的小型传感器到复杂的工业控制系统（集成电路）。最终，该设备直接或间接通过与一个机械装置相连的方式对物理世界产生动态影响。

物联网设备一般有三个共同的属性：

（1）普通对象是可以检测到的，这意味着在网络中的这些对象可以单独寻址；

（2）这些物理对象是相互关联的；

（3）无论是自身或与其他设备或应用程序的组合（基于其编程或编程与物理世界收集的输入的结合），这些设备都表现得非常智能且能自适应调整功能。

在政府、工业和私人生活的基础设施部门中，许多类型的设备正在被快速设计用于发现一些物理现象（例如，运动或指定的热或光）。当满足特定的条件时，这些自适应设备能在未经人类或其他计算机的进一步的命令授权情况下会自动执行所设计的功能。这样的设备还可以使用物联网设计中固有的通信连接来接收远程命令以执行特定功能（例如，打开（或关闭）开关、阀门或操作机械设备）。

物联网的概念比较新，并不是简单地把电脑连接到机器上去。工厂和机器设备长期以来一直由工业控制系统（ICS）和监控采集系统（SCADA）控制和管理，他们负责基于操作环境对工业和机械进行监测和控制。这些物理设备连入互联网并非是革命性的，使得物联网不同于传统信息技术是它在下面三个方向的爆炸式扩张：

首先，物联网的部署规模和应用的速度是前所未有的。虽然和传统的行业

有所不同,但是它很快被大众广泛接受,仅仅5年时间,就有260亿至500亿物联网设备被部署。相比之下,发展超过一代人的手机发展最盛时期使用量也只有六十亿。

其次,物联网的部署范围广,大到非常复杂的系统,小到简单的设备,从主要生产设施和控制中心到消费者。

最后,物联网部署的人口跨度也正在迅速蔓延,没有基础设施不受到这种现象的影响。

物联网涉及美国社会的方方面面,它将创造未知的网络连接和依赖关系。水力、电力、紧急服务、医疗保健、农业和运输业等行业越来越多地依赖于物联网设备。这将创建一个环形的设备依赖网络。同样地,物联网设备本身是依赖于一系列的其他物联网设备来提供必要的服务,如电力、通信和数据服务等。

无论那些面向消费者的平台或系统是否直接连接到NS/EP系统,物联网都将直接影响到NS/EP系统,在联邦和与安全相关的组织和基础设施领域的所有工作人员将受到物联网爆炸式发展所带来的影响,最终影响到每个消费者的日常生活。这种影响是不可避免的,并且任何的努力都不足以阻止它,即使试图以安全的名义,也不可能完全解决。INTAC向总统报告政府安全通信的时候,NSTAC指出了现代信息技术已经广泛被工作人员接受,并应用到NS/EP相关的工作中,悄然改变着非机密政府工作的安全性。该报告的调查结果、结论和建议已经被新的物联网现象验证。物联网的快速部署导致风险正在不断增加,那些正在被广泛使用的能产生巨大效益的新技术亟须新的方法来保证安全,同时,工业物联网的基础系统设置也应该采用新的方式,此前的方案中,系统可以同时被授权用户和恶意用户访问和控制。综合起来,物联网已经广泛扩散到各个消费领域,已经渗透到传统独立的工业环境中,并将成为不可分割的一部分。

物联网的快速应用创造了很多即时的、真实的利益。那些通过网络连接的设备可以更有效、更稳定地运行,因为它能在潜在故障发生之前进行自我报告。连接的医疗设备可以很好地检测病人病情;先进的物流可以提高零售商的分发商品的能力,同时能提高联邦应急管理机构的灾难响应能力;普通民众也可以通过物联网技术简化和改善他们的生活。

与此同时,物联网也会带来很多风险。对于个人消费者来说,风险往往是次要的,商业物联网设备的沦陷可能造成些许不方便,但一般不威胁生命或国家安全,然而,医疗器械,包括那些可植入的器械会因为他们内置的连接而和传统的器械显得不同,物联网医疗设备的故障可能会导致病人的死亡。DNI在2014年1月国会的声明中指出:"个人设备、医疗设备和医院网络的交叉部署,网络的漏

洞可能会对患者导致意想不到的结果”，物联网也增加了个人隐私的风险，因为大多数的物联网设备都会对用户数据进行采集、分析和存储。

同时，运行或连接到国家关键基础设施上的物联网设备的故障也会对国家经济和安全造成影响，关键基础设施中物联网设备越来越自动化，且自适应能力越来越强，它们可以控制系统、收集数据，并作用于这些数据，一旦这些设备发生故障，将会造成非常深远的影响，这些影响可能是经济层面的（例如，生产力和对国民经济的损失）或在公共安全领域的（例如，动态损坏或在极端情况下机械或基础设施发生灾难性故障）。

尽管一些技术人员可能预见到这种缺陷，但是物联网的爆炸式增长以及不同系统之间不断增加的连接性未被考虑到当前网络系统和机械的设计中。结果就会带来一些与 OT（operational technology，运营技术）和 IT 较差连接性相关的网络安全风险，他们的交集有时称为冲突或收敛。

IT 和 OT 在历史上就是响应不同的需求的，从风险承受能力的发展过程来看，有着完全不同的基本计划和假设。例如，IT 领域相关的设备和软件的寿命可达数月或数年，而 OT 的生命周期往往可以达到几十年，从历史上看，IT 和 OT 在学术界和研究机构常被视为独立的学科，为了尽量减少由物联网带来的潜在风险，这种差距必须解决，这要求从一开始就必须要考虑到安全性和应变能力的问题。

物联网也开始打破商业和工业技术之间的壁垒，那些旨在面向消费者的设备和软件越来越多地被用于制造业和国家安全行业，此外，有可能某些被消费者广泛青睐的低功耗、廉价的设备和技术，包括应用软件等也可以和基础设施系统联系起来，作为更复杂的关键技术产品的基础。因此，在面向消费者设备的背景下做出的安全决策和引入的安全缺陷可能比先前的创新具有更深远的影响。

B.2.3　NS/EP 中物联网影响的思考

物联网技术的快速部署，也潜在地影响国家安全和应急准备（NS/EP），从关键服务如何交付给公民到如何保护国家都存在着问题。IoT 设备的广泛使用允许扩展态势感知和数据分析，这将增强基础设施运营。显而易见的，在智能城市、智能电网和智能交通等领域，以及正在向个人、大型企业网络推出的无数智能设备中创新和部署的速度似乎没有放缓。

向公众开放的高度集成的物联网环境有望促进经济发展、改善公民的生活。当 IoT 与其他相关技术概念（例如，大数据、云计算、机器人技术和自主性）相结合时，IoT 将为不同需求的用户产生前所未有的效果。但是，也有其他因素可能

阻碍物联网达到其最大潜力,具体包括未能管理与快速创新和增加连接带来的风险,缺乏一个权威的支持结构,以及政策和治理方法无法跟上物联网技术发展和部署的速度。

1. 物联网技术的独特之处

物联网时代可能是互联网革命中最具颠覆性的时代。物理对象、远程存储的数据和自然环境都将相互交互。尽管对物联网技术提供的巨大潜力已经达成共识,但人们似乎普遍缺乏如何保证在最大化物联网对于NS/EP潜在利益的同时确保适当的风险管理的远见和目标。此外,当前的治理流程没有和物联网创新相关的变化步伐保持一致。IoT设备的数量不断增加,由于物联网技术的模块化,暴露了许多标准化、互操性和身份验证相关的空白。

2. 物联网设备的扩散

物联网产生的缺口增加了一些设备不被网络检测到的可能性,从而使得难以保护它们免受不法分子攻击。因此,不法分子的攻击面呈指数增长。此外,许多面向消费者的设备和工业设备依赖于最初安装的嵌入式处理器,在设计初期并没有考虑到将它们连接到网络;然而,现在的建筑物供暖、通风和空调系统,制造系统以及汽车制动和转向系统都能够提供进行远程监控和远程控制的接口。随着物联网设备的使用变得越来越普遍,机构和组织已经难以避免依赖物联网源头和产品提供的功能。对比移动通信的发展历程,智能设备的普及趋势也将变得不可避免。随着这些设备的不断增加,重要的任务是保证信息安全,减少未来的风险。需要明确的方案来帮助那些机构和组织在采用新的物联网技术或将物联网应用到传统系统之前做出安全决策。

白宫总统创新研究项目,也称智能美国项目,展示了整个城市和经济部门(如交通运输和能源)如何融合新兴物联网技术的益处 。该项目展示了物联网的巨大潜力,但同时强调了以下两点:①物联网的功能和设计文化使其进入市场的速度超过任何安全问题;②目前没有公认的库、信息交换流程或权威组织来为它们提供经验教训,以便物联网能够轻易地部署。

3. 废弃数据

已部署的数十亿个联网的智能设备正在产生越来越多的数据,这些数据可以以多种方式使用。新的数据来源的意想不到的后果是会产生“数据废气”,当被恶意分子检测到时,重要的数据(例如,国家领导人的地理位置或生物特征)可能会被截获。物联网设备收集数据的潜在影响是无限的。

在物联网出现之前,数据收集是在封闭的仓库中进行的,数据倾向于保存在其原始单位或组织中。物联网的普及改变了这一点,数据聚合和数据的广泛使用现在已成常态。面向企业和消费者的数据聚合服务使得物联网设备生成的大量新数据的挖掘变得非常宝贵,但它们也将成为攻击和隐私侵犯的焦点。我们可以通过优化流程、资源分配和决策产生巨大的社会效益,其中,在关键基础设施的一些部门,包括健康、能源、交通领域已经实现了早期效益。另外,物联网引发的数据爆炸(通常称为大数据)虽说不是新兴的,但物联网数据分析将推动新的生产、发展和创新浪潮,最终影响每个部门。然而,挖掘大数据的全部潜力是极具挑战性的。此外,数十亿的设备每时每刻产生数据,进行数据传输和并存储数据,最终将导致数据废气,这可能将产生不容易发现的漏洞。通常这些数据包含很多敏感信息,诸如遥测、语音、视频、健康和基础设施组件的状态数据。隐私权法、安全法、知识产权法和使用条款将需要更新来适应这一新的现状。

同时,需要更多的专家来充分利用物联网提供的数据,组织可能面临大数据使用优化的挑战,包括了解现有的控制机制,以保护数据传输系统、处理系统和存储系统。由于某些组织和代理机构尝试整合来自多个数据源的信息,对数据的访问变得越来越重要。

4. IT 和 OT 网络的角色和功能模糊

物联网模糊了 IT 和 OT 的边界。多年来,IT 和 OT 已经发展了自己的一些支持者、价值观和用户文化等,最重要的是,IT 和 OT 开发了几乎完全不同的方法来保证安全:IT 安全主要通过打补丁和频繁更新的方法(需要使系统脱机的能力),OT 安全主要围绕着模糊和专业化(系统需要保持在线,来判断是否受到影响)。在物联网中,这些领域动态地交互。

认识到 IT 和 OT 在设计和用户社区模糊地传播,IT 和 OT 从业者基于自己的考虑和经验,试图说服他们的同行需要适应他们的产权、文化和使用方法。证据表明,无论是赞成任何一种观点或达成平衡,这些努力几乎没有取得了任何进展。由于物联网(无论其特征主要面向 IT 还是 OT)继续沿着爆炸趋势扩散,需要一种新的范式来描述,其中 IT 和 OT 被认为是一个集成的单一概念。随着时间的推移,IT 和 OT 系统在物联网内部相互作用,它们越来越多地呈现彼此的某些特质,变得不能清晰地定义为“纯 IT”或“纯 OT”。技术将引领着技术运营商倾向于扩大设备使用的界限。

为了理解与 IoT 的关系,重要的是要认识到设备如何使用的相似性和差异性,而非判断设备是否属于 IT 或 OT。在许多情况下,单个技术或系统可以用

于许多不同的目的。例如,现代的台式计算机可以专用于支持制造功能,并且只要它与较大的 IT 环境隔离,它就可以在更长的时间段内安全和有效地工作;然而,如果该设备连接到互联网时候,该设备的操作者必须认识到需要接受与 IT 相关的安全原则和实践。从网络安全的角度来看,与互联网连接的机械设备变得容易受到和互联网相同的攻击和漏洞利用。

物联网设备趋向于有目的的设计和不同领域的机械设备,旨在跨越经典的 IT 和 OT 功能,清晰地证明其是否属于 IT 或 OT 变得无意义或不可能。如果不能根据现有规范对这些设备进行分类,那么可以认为,该技术自身就是一种学科、一种混合技术。

认识到设备的混合特性提供了许多优点和新的视野。在基本使能技术和设计的水平上,其中共性是最大的,可以定义和描述最有益于安全的标准和设计元素,通常包括在本地网络上使用基于 IT 的标准安全包,网络端口安全技术或入侵检测技术,通过这种混合安全方法,为物联网领域实现广泛利益提供最佳机会。混合安全机制的目的是识别和处理所有 IoT 设备共有的安全问题,而不管部署领域或最终用户,这将允许终端用户和应用程序管理员专注自己领域的威胁和需求。这种混合安全机制将作用于许多设备和系统的整个生命周期。事实上,IoT 将会逐步发展起来,并在人口统计上比那些在某些领域已经发展很好的纯 IT 或纯 OT 更快地扩展。对于这些物联网设备,常见的安全措施将带来最大的好处。

站在终端用户和系统部署的层面上,无论是制造业或 IT 网络运营业,为了满足不同用户和运营商的需求,许多设备都采用特定的应用程序和特定的设置。这些领域特定设备的安全机制和其他管理决策不会因为出现混合技术而改变,除非随着时间的推移,物联网技术能在关注安全中获益,那么管理者有可能会接受它。为了 NS/EP 的目的,可以在确定感兴趣和责任范围内的 NS/EP 领域中部署和定制混合安全标准和实践。例如,在灾难响应中使用的 IOT 设备将具有与在战斗区域中使用时不同的实用性和安全需要。安全机制应适合于设备和特定用例。

在操作环境中,终端用户组织最后通常是选择适应新技术,因为技术的全部效果最终会得到实现、认可和评估。在这种情况下,紧急需求是混合安全机制的重点。由于这些技术完全是 OT 和完全是 IT 的,而不是排他性的,因此创建管理环境和方法非常重要,这些管理环境和方法将工业和网络运营的所有需要的考虑和文化引入到安全标准和实践的开发及管理中,用于核心混合安全技术。

5. 不断演进的 IoT 生态系统的安全性

如前所述，物联网将对 NS/EP 产生广泛的影响。庞大的部署规模和设备之间无处不在的连接可能导致在响应用户需求之前发生迅速的级联事件。生态系统的每个元素都会引入额外的安全风险，而且物联网设备的部署速度要快于这些风险的可理解程度。在这种环境中，强调集中控制或侧重于单个系统的网络安全处理已经不足以解决物联网的安全性和灵活性。物联网创造了对端到端生态系统实现安全性和弹性的新方法，其中可以以分布式进行自动决策，并使用约定的原则，实现实时响应 NS/EP 事件。

（1）信用

信用涉及从设备和系统到数据和算法的整个物联网生态系统。它还包括需要一致和可靠地执行一定级别的安全机制。可靠性将随设备和使用的变化而变化，但 NS/EP 应用需要最高级别的保证。在分布式环境中，需要通过每个 IOT 开发者、程序员或安装人员进行相应最佳实践、原则内化并不断熟练来实现。这意味着在开发和部署物联网生态系统时，需要将安全处理推向生态系统的每一个可能发生威胁的元素。纵深防御通常是一个合理的行动方式，系统始终秉持“不信任并始终验证”的原则（即系统不应该信任接收的数据，并且总是对任何连接验证），这种思想应该被集成到物联网生态系统的设计，这一点在 NS/EP 应用中显得特别重要。

相关人员应考虑以下做法，通过调整现有的安全设计最佳实践和网络安全来加强物联网安全：

① 最大程度地减少已知的漏洞并降低新的物联网设备带来的安全风险

物联网设备的功能差异很大，从简单的传感器到复杂的系统，潜在风险不断变化。这些不同类别系统的设计、开发和制造中的设备分类和最佳实践有助于在其整个生命周期（包括生产周期）中最大程度地减少已知漏洞。设备应尽可能设计为未来兼容，并纳入未来任何生态系统升级的不可缺失的一部分。这些机制可以根据不同类别的物联网设备和用于最高安全级别的 NS/EP 关键功能的设备而变化。有权限设备可以周期性地发送升级通知，或者能够学习新的算法以改进其处理方式。

② 识别和评估现有 IT/OT/IoT 部署的安全漏洞，并为 NS/EP 制定合适的威胁模型

应该在 NS/EP 网络全部范围风险上部署和测试这种威胁模型，包括依赖性和人机交互界面。在公共网络上越来越多地使用不安全的个人设备连接到公共

基础设施网络中，这将会产生更高的风险，物联网设备的普遍存在更加证明了进行用威胁模型分析的重要性。

③ 为具有潜在 NS/EP 影响的数据进行分类以实现额外的安全保护

大多数 IoT 设备通过 Internet 或其他不受保护的网络运行，其中许多网络的存储和处理能力有限。结果，数据需要传输到中央节点进一步处理，这增加了数据被破坏的机会并且加剧了数据泄露的潜在威胁。相关人员应制定合适的数据分类，确定出具有不同保护等级的物联网数据。

④ 创建行为和功能透明的 IOT 系统

具有 NS/EP 影响的 IOT 设备和部署的系统应该具有良好的理解、良好的文档或可观察的特征、功能和相互依赖性。

⑤ 开发可以共同使用的安全和信任框架，以实现威胁信息共享

IoT 可以提供详细信息来预测和防范攻击。例如，来自多种类型的传感器的信息可以用于高级自动化威胁诊断的数据。这将需要可以共同使用的安全和信任框架来实现协作，特别是在司法管辖区之间。

⑥ 探索新的 NS/EP 安全模型，特别是在生态系统层面，实现可自主、快速和规模化地做出安全决策

物联网的活力为现有安全实践引入了新的适应性要求。例如，作为安全设计的一部分，组件和系统必须能够动态地学习和检测新的漏洞，并且如果必要的话，需要隔离自己。此外，对单个组件或系统级别的安全性检查已远远不够了。由于物联网的连接无处不在，在数据生态系统中探索威胁检测并实现端到端安全的技术也显得至关重要。最后，由于 IOT 设备动态变化的能力，可能需要它们彼此协作以为整个系统提供恰当的安全级别。

（2）弹性

政府和其他行业必须对支持 NS/EP 功能的物联网系统的风险进行管理。由于物联网刚刚兴起、部署非常快速、设备应用的广度和多样性、实际和潜在供应商的数量庞大以及缺乏技术标准和操作程序等因素，物联网的安全性仍然特别难以管控。因此，物联网的安全性在部署之前不可能在短期内确定，政府应制定应急计划，解决联邦部门和机构中物联网的部署问题。对不安全环境的综合规划应再考虑一些其他的技术概念，如上述的可升级性，以及其他技术，包括架构（例如控制平面和管理平面分离）以及政策和规划工作（例如，更新操作的连续性/政府的连续性），都应该升级更新以提高弹性。

在事件的早期阶段，可能难以确定是否发生网络攻击或故障。物联网需要从响应检测保护转变为强调生态系统的生存能力并最小化对物理系统的负面影

响的模式。生态系统的弹性对于具有潜在 NS/EP 影响的物联网系统尤其重要，单一或一系列攻击都不应该导致生态系统的灾难性故障。即使某些系统受损，生态系统都必须保持运行。

为此，物联网系统应当利用当前在线服务中使用的策略。例如，系统开发人员和管理员可以部署测量和报告的方法，收集和分析给定 IOT 网络的关键性能指标。这样的过程对于应用 IOT 的扩展层面是至关重要的，因为它将有助于减轻系统产生的级联失效，其可以包括许多自适应部分并且可以不涉及与人类交互。

在生态系统中共享关于物联网相关事件的信息也是非常重要的。在一个互连的环境中，系统独立地做出决策，这将造成对较大网络造成风险的结构性问题。诸如信息共享的过程可以准确定位系统损害的地方，并且能预先做出调整。

(3) 个人

个人行为在任何安全框架中都至关重要；然而，由于物联网设备和 NS/EP 考虑的结合，使得这种情况更加恶化。总的来说，主要来自两个方面的挑战：生态系统的互联性和扩大的攻击面。因此，任何设备都可以成为进入生态系统的潜在来源和增加态势感知的机会。在这种广泛分布的系统中，个人对威胁和风险的认识以及安全设备的使用是风险缓解处理的一个基本要素。同时，消费者的需求也可以推动市场需求走向更高安全标准的物联网设备和服务。

(4) 与工业界合作

凭借物联网带来的巨大经济机会，包括制造、能源、交通、通信、零售、医疗保健和城市发展等众多行业在发展物联网创新方面均处于领先地位。随着公司认识到需要开发可互操作的平台和系统，形成了多个行业联盟（例如，开放互联网连接联盟和工业互联网联盟）来解决生态系统和不同部门的不同问题。政府需要利用这一创新和最佳实践与私营部门合作，解决物联网对 NS/EP 的影响。

(5) 物联网系统的自动化和自适应特性

物联网系统是端到端的，不仅包括传感器和设备到网络的物理连接，而且包括用于分析数据的软件、系统和算法。这些系统还包括通过预先编程或机器学习算法，由对象展示的许多自适应行为。虽然这些是自动化的，但是它们的功能可以基于机器学习算法进行重新配置，在某种程度上引入了不可预测性。各种 IoT 文献将这些系统描述为自主系统。物联网在这一方面引入了影响 NS/EP 的附加威胁因素，因为系统可以被重新编程以通过特定的数据输入或与其他系统的交互来自动改变它们的行为，其产生的影响可能是积极的（例如，对威胁或事件更快的反应），或者也可能是消极的（例如，可能发生难以控制的级联效应）。

在最坏的情况下，这样的系统可以比人类参与更快地引起或加剧威胁 NS/EP 的事件。

6. 物联网治理注意事项

适当的治理，特别是通过公私合作关系发展，对于确保大规模系统的互操作性和一体化至关重要。最近国家标准研究所(NIST)网络安全框架和为第 44 届总统拟定的网络安全委员会报告就是一个比较好的例子。物联网将同样需要治理并且也需要这种公私合作关系，但是需要特别紧迫，因为这是物联网设备的快速采用和这种现象对 NS/EP 影响的结合。物联网需要比规范更快地制定治理和政策结构。此外，由于物联网是全球性的、无边界的，良好的治理需要国际参与。

(1) 政策审查周期

技术通常比政策发展更快，这使得在技术现状和政策发展之间会存在空白；然而，物联网比以前的技术发展更快，这种差距显得更大，渐渐变成一条不可逾越的鸿沟。例如，隐私问题就是因为数据采集增加和新技术部署引起的，但却没有关于安全性和用户隐私的相关的已建立的政策。

如上所述，预计未来几年内，物联网的使用将达到 500 亿台机器和设备。这类似于 1994 年蜂窝移动业务的状态，当时蜂窝移动电话被广泛使用，但仍然不可能预见未来的变化；而类似地，物联网的使用将明显快于手机的使用。政府仍在努力制定政策以解决手机使用的增长，而物联网政策已经远远落后。重要的是，许多提供与网络安全相关的战略方向的国家级文件没有涉及甚至没有提及物联网。政府必须迅速采取行动，解决这项技术将带来的威胁和脆弱性，鼓励物联网创新，实现持续的经济增长。

随着国家政策滞后，政府不能依靠现有的政策发展机制，而是必须寻求新的方法，比如利用私营部门获得的知识，特别是有关新兴先进技术的知识来制定物联网政策。政府可以通过召集专家建立联盟或机构，为联邦政策以及私人安全最佳做法和管理方法提供指导，从而实现最好的效益。此外，由特定利益群体组成的现有财团应考虑跨部门合作，并接受企业级与国家安全的顶级架构指导。政府在促进这种跨职能工作方面具有独特的优势。对于物联网，有效的方法可能是通过关注案例研究，提供关于 IOT 如何在不同行业得到解决的最佳实践和成功案例，然后评估对 NS/EP 的影响。

(2) 治理结构

国家网络环境的安全需要基于共识的标准、最佳实践以及在各种环境中应用的指导。这些将需要与可信和有价值的信息共享协作机制相结合，以便尽可

能快地识别和应对不可避免的缺陷。至关重要的是，政府必须建立一个权威的机构，同时，应该利用相关领域的专家进行决策来应用网络安全的已知标准、实践和其他准则。NIST 负责为民事部门和机构制定和应用联邦计算机安全标准和方案，国家安全局负责国家安全部门、机构和系统；然而，私营部门没有类似的信息系统安全联络点。事实上，有许多从事网络安全领域的公司和组织为业主、运营商和用户提供建议，这些公司和组织对许多用户和中小企业来说是几乎不可见的。

2013 年 2 月发布的行政命令(EO)13636 号文件《改进关键基础设施》已成为私营企业和公共部门合作开发网络安全框架的协调中心之一。由 NIST 制定的安全框架为将风险管理实践和现有网络安全与隐私标准应用于一系列操作环境提供了广泛的指导。

然而，该安全框架并不为具体情况提供细节指导，而是由选择使用它的组织掌握。一些部门组织已经开始根据其部门的需要填补这一空白，但这也将需要每个组织稳固其自己独特的系统。

这些努力正在网络空间领域取得一些成就，但进展缓慢。然而，如今的网络安全环境表明，如果在部署物联网早期未考虑安全性和隐私，那么之后考虑安全将更加困难和且付出的成本更大；相比之下，提前考虑到安全性则可以节约很多成本，并且在早期考虑和规避那些不可避免的风险，往往会有更多的设备选择余地。一个鼓励生产和采用网络设备与系统的强大的私营部门主导机制，可以提高国家的安全和隐私。

(3) 隐私注意事项

现有的数据隐私标准和概念不能很好地转化到物联网环境中，物联网环境中由于无所不在的网络连接，数据的可访问性可能已经扩展到了多个相关的社区，数据生成设备的激增具有显著的益处，但也易受恶意破坏或其他未预料到的影响。

Hewlett-Packard 最近的一项研究发现，90%以上的物联网设备都至少收集了一条个人信息。在这些设备中，80%的设备未能使用足够的身份验证。此外，70%的测试设备在传输此数据时不使用加密，从而该设备下载的数据可能被拦截、查看和修改 。传感器可以聚合个人的大量数据，对于营销和企业工作以及医学和行为研究等具有巨大的价值。

然而，也存在更多恶意使用数据的案例。当没有感知或同意收集数据时，人们可能不知道企业和政府可以得出的关于他们的生活、习惯等各种的数据；此外，当数据大规模聚合时，看起来无害的数据元素可以被组合成前所未见规模上的身份盗窃。同时，聚合的地理位置数据也使得个人，包括国家领导人被跟踪。

隐私设计是解决这些问题的一种方式。隐私设计是在项目启动时建立的隐私管理方案,允许在收集数据时匿名化数据,并向用户提供有关收集的数据及其对该收集的数据的控制信息。通过对收集的数据匿名以保护隐私,同时有利于其他聚合分析。应急救助人员、交通工程师和其他组织可以使用这些数据来惠及整个社会。

用户隐私与NS/EP有着重要的联系,这个问题正通过其他领域隐私研究和举措得到解决。NIST已经开始实施隐私工程计划,有助于从面向过程的原则(如与公平信息实践原则(FIPPS)相关的原则)转变为风险管理框架 。这是政府和私营部门合作制定治理规范的一个极好的例子。

(4) NS/EP通信的弹性和优先级

国家安全、应急准备、关键基础设施和关键资源(CIKR)用例的NS/EP通信由于物联网的发展滋生出许多独特的能力和挑战。现有的NS/EP通信服务,包括电信优先服务(TSP)、无线优先服务(WPS)、政府紧急电信服务(GETS)和特殊路由接入服务(SRAS),都需要重新考虑物联网的独特属性。政府需要处理的一些问题包括:

如果IoT设备连接到有线或无线网络并且NS/EP扮演重要的角色(例如传感器/处理器),那么该设备如何验证并接收网络优先级?是否应该验证?

TSP优先级供应、恢复和SRAS中继分配是物理的、基于电路的平台和技术,因此,如何建立和维护与IoT端点的连接?如何设置优先级?

虽然在下一代网络优先服务(NGN-PS)中考虑了数据服务,但是如何评估在NS/EP功能中运行的自适应的处理器和传感器的独特属性?

考虑到通信技术迅速变革,政府提出了《国家安全和应急通信职能分配指令》(EO 13618),该指令指出:国家安全和应急通信执行委员会的职责是,通过PPD-1程序向总统提出可行建议并推荐有效政策,以提升NS/EP通信的生存性、弹性和未来架构,包括应构成NS/EP通信要求的内容。

通过一种基于IP协议的网络技术提供端到端语音、视频和数据服务的通用通信的演进为确保现有NS/EP优先通信程序的功能创造了新的机会和挑战。随着通信行业发展,技术不断改进,运营成本不断降低,提供更大的带宽和更多的网络服务,政府仍必须履行EO 13618中关于国家领导人、联邦、州、地方政府和其他授权的NS/EP用户的责任。现有保护程序首要目标是在网络拥塞的情况下为NS/EP提供网络恢复和更好的网络访问。

关于NS/EP电信优先服务及其相关联的身份管理架构,IOT设备目前无法利用现有或计划的GET/SRAS个人识别号码验证的NGN-PS功能,但是可

以使用 WPS 订阅。为了支持物联网,政府应审查 NS/EP 政策,包括对设备、终端进行 NGN-PS 授权、会话建立、认证和终止。

国土安全部紧急通信办公室(OEC)已经建立了一个合同机制,支持 NGN-PS 解决方案以应对物联网等挑战。为了进一步研究如何将物联网纳入优先服务,NS/EP 通信执行委员会和 OEC 应扩展 NS/EP 通信要求,检查物联网的影响,包括设备、终端 NGN-PS 授权、会话建立和认证等所有方面。

在这方面,物联网的一个主要驱动力是制定开放的、自愿的和基于共识的标准。正在进行的和未来关于标准化的努力使物联网成功将贯穿整个市场,并将涵盖从总体方案到具体技术标准,确保增强的互操作性以及向后兼容性。重要的是,这些标准能够根据相关人员的专业知识,动态地适应需求的变化。许多解决行业共识需求的标准化努力,以及未来的努力,将有助于可互操作的物联网的发展。这些标准化的努力为政府提供了一个机会以加快物联网在国家安全、应急准备和 CIKR 使用案例中的发展。尽管不是特定于 NS/EP 通信,但诸如电信工业协会研究标准 TR-50 机到机(M2M)(智能设备通信)的标准化努力是一个很好的示例。另一个例子是 one M2M,致力于开发技术规范,以解决对可以容易地嵌入在各种硬件和软件元素中的公共 M2M 服务层的需求,以及许多其他的需求。

标准化是一种经济自律的形式,可以减轻政府制定详细技术规范的责任,同时确保自愿的、协商一致的标准符合公共利益,节省可用于以其他方式为公众服务的资源。通过采取这种方法,政府决策者可以在私营部门专家的协助下使用标准作为科学和技术信息开发的宝贵来源。组织机构还可以使用这些标准作为高级技术信息的资源,而无须该地区研究的第一手资料。

物联网将显著依赖于最大化连接的连续性。此外,随着世界连接的方式迅速变为无线,建立适当的频谱策略对于确保物联网的安全至关重要。无线连接正在成为消费者接入因特网的方式,主要技术有 LTE、Wi-Fi 和卫星技术等。传统 Wi-Fi 也会因为其低成本和在市场的广泛使用而在物联网部署中发挥关键作用。有效的风险管理将需要仔细检查网络连接,以确保其安全性和可靠性。在检查用于 NS/EP 通信的物联网系统的风险分类时,确保考虑适当的网络技术至关重要。包括使用许可的无线频谱、优先级(QoS)与最佳效果连接、有线与无线,私人线路的虚拟专用网络与公共网络。

未来物联网将可能基于异构网络,由此设备可以顺序地或同时使用有线或无线网络技术。这也抛出了另外一些话题:如何通过网络去度量 NS/EP 物联网通信,可能需要一些措施去保障 NS/EP 物联网通信。

7. 物联网机构支持与结构

物联网部署的步伐以及对美国社会的影响突出了对物联网对 NS/EP 的影响，需要制度和程序来使得物联网技术的潜在利益得到保障并最小化风险；然而，这种制度程序到今天没有充分确立。仍然缺乏对 IoT 这个术语的共同定义和理解，未能产生协作的工作流，物联网未得到充分了解，其影响未得到广泛认可。物联网的教育、培训和认知不成熟，研发不协调，没有统一的与 NS/EP 用途相关的国家优先级。在美国，物联网的发展影响着全球研发和标准，并受其影响。

（1）在 NS/EP 背景下的物联网教育、培训和认知

虽然物联网是一个相对较新的术语，但在 NS/EP 背景下，人们对于 CPS、ICS 和 SCADA 系统相关的教育、培训和认知特别感兴趣。ICS 和 IT 系统的集成造成了缺乏训练有素的同时具备 OT 和 IT 技术的综合能力的专业人员，因此教育计划也应该升级。

学术界正开始将 IoT 和 CPS 概念引入工程、计算机科学、信息科学、数据科学和网络安全相关课程，但是，项目还处于早期阶段。值得关注的是，随着物联网的不断出现和扩展，操作的复杂性越来越高，因为处于退休年龄的工作人员超过了在工程领域的美国学生的比率，了解工业领域复杂系统的人大量退休，同时工程学位的学生入学率正在下降。

在美国大学的研究人员和研究机构的专家正在研究这种不断发展的技术对网络安全的影响，NIST 网络物理系统公开工作小组也是如此。可利用国家对网络空间教育(NICE)劳动力框架倡议，进一步引起全国对物联网机遇和挑战的关注。NICE 组件 1：国家网络安全意识领导：DHS；组件 2：正式网络安全教育共同领导教育部和国家科学基金会都是已经实施的方案的示例，可以升级这些方案以创建更强大的教育和认知方案，包括物联网在内。

许多特定业务部门(包括运输和电力)的网络安全专家认识到新兴物联网技术的优势和其在关键基础设施部门的潜在脆弱性；然而，一些人没有对物联网完全感知，可能更加热衷于物联网技术的新功能，并且不了解其可能带来的风险。因此，需要从许多层面提高公众对物联网的利益和风险的认识，无论是公民还是国家立法者，对领导者和决策者来说，了解使用物联网技术的影响尤为重要。在联邦机构，许多物联网相关的工作正在进行，特别是那些与移动网络连接的部分；然而，它们没有出现很好的协调，以分担与物联网相关的安全隐患。此外，没有用于收集或分享有关新兴技术的经验教训的资料储存库(在政府或各个行业中)，这种资料库对于制定 NS/EP 系统的协调方案是有用的。

虽然物联网涉及的技术很深奥,但物联网对用户来说是友好的。政府员工和公众在使用物联网设备的时候,通常不用了解或关心支持设备功能的技术细节。上述物联网面临的挑战是非常复杂的,因为用户不可能知道与新功能相关的风险,直到有人受其影响。物联网创新的功能会激励买家的购买欲望,然而,当越来越多的消费者了解和意识到物联网的风险后,他们就会帮助推动市场采用更好安全性、更好隐私性和弹性的物联网标准和解决方案。

(2) 研究与发展

不同于已建立的架构,它的设计和操作都已经被很好地记录,物联网还在进化中。单个的物联网技术和系统已经存在,但目前还没有基于标准化的、国家安全系统支持的大规模的物联网的部署。尽管物联网有巨大潜力,在某些技术有重大进展,但是美国仍然缺乏一个集成的视角来实现集成的、基于标准的物联网系统。

在系统层面的物联网研究仍处于早期阶段。目前的大多数研究发展在相对狭窄的、工业和学术界的特定场所。这种研究通常被划分为传统的学科,如传感器、通信、操作技术和能源效率。职工教育和专业知识的以相对的零散状态存在,这些因素给未来的物联网系统的设计提出了一个艰难的挑战。

为了构建一个无处不在的、可靠的、安全的大规模互联的物联网系统的视角,确保被个人、组织、市政府和政府的广泛接受,连贯的符合国家战略的多学科研究是一件很有必要的工作。一些关键的研究领域涉及物联网架构,包括标准、识别、安全、隐私技术以及实践和网络管理技术。

① 物联网架构

对架构、接口和整合的无缝架构的接口和网络、传感器、控制以及计算的抽象的创新方法,以及异构的物联网系统部署必须被快速开发。例如,在通信网络,接口在不同的层之间已被标准化。接口的抽象,使得每一层的部署独立于其余部分的系统。这个方法允许系统由独立开发的组件、开放的创新机会和快速扩散的机会以及发展的互联网组成。在物联网空间,已有的工具、做法和标准不支持常规的模块化设计和发展。标准化的架构、接口、模型和抽象要求支持敏捷开发、认证和验证、互操作性以及物联网系统的创新。全球的物联网性质指出,需要的标准,包括分层的或可扩展的信任级别。此外,在传统的设备管理,特别是在工业环境中还需要进一步的研究。一些现有的物联网设备,特别是在曾经的工业环境中,很少重新启动或修补。研究是一种必要的安全保护技术来保护这种长期运行的设备。

② 标准

标准提供一个基本的互操作性,它是物联网的价值命题的本质。有几种类

型的互操作性,包括技术、句法、语义、组织、静态和动态。所有的这些互操作性的形式要求有效地把物联网集成到 NS/EP 系统和操作中来。

物联网技术支持的 NS/EP 系统应基于开放式架构来最大限度地提高异构系统和分布式资源之间的互操作性,这些资源包括信息和服务的供应商和消费者,不管是人、软件、智能对象或设备。因此,标准组织应为物联网系统制定通用的 NS/EP 安全参考的模型、体系结构和接口。

定义技术和掌控互联以及信息传递接口的逻辑状态标准将需要被采用,来符合所需的互操作性水平。标准将需要数据编码的开发,空气接口,测试,安全性,功耗和功耗,安全性等其他功能。联邦政府将需要参与到标准设置组(国家和国际)来促进支持 NS/EP 识别的物联网系统标准的发展。

③ 身份验证,安全和隐私技术以及实践

全球通信网络正在不断发展,以适应新兴的物联网技术的发展。然而,在全球范围内对技术操作性的识别和认证技术的进一步提高的研究是必要的。

隐私和保密性问题的研究,以及身份和匿名部署的技术测试是很有必要的。例如,一个设备可以被证明是一个没有被揭示的独特的身份性质组的一部分。同样,该技术可以用来验证一个人是一个小组的一部分,而不用透露身份(例如授权驱动程序)。也应该进行适当的证书管理机构的探索。

未预计后果的相关物联网系统的部署可能会导致大量的数据产生许多不同的来源,并增加内部连接和数据保留。在物联网环境中,每一个节点都可以连接到全球互联网,并能够与其他节点进行通信,这也会创建新的安全和隐私问题,如数据收集的保密性、真实性和完整性以及物联网网络的交换。

④ 网络管理技术

与国家生态系统交互的物联网网络的设计和实现提出了几个挑战,这些挑战与实时操作,可靠性、安全性、应用以及异构系统的互联互通有关。物联网网络管理系统必须监控参数,如交通流量和大规模实时系统和系统的拥塞、稳定性和可用性安全。网络管理技术将需要对潜在的网络上可见并检查运行在其上的进程,无论设备、协议或地理位置。一个特别的研究重点应该是在使用在网络操作优化和网络攻击检测上的预测分析。

(3) 国际影响

物联网是一个全球性的现象,需要全球参与研究和开发,并标准化地发展。美国需要积极参与国际活动,以跟上步伐和领先的进步和不断发展的标准。

如前所述,物联网以加速的 M2M 业务带来全球影响力的提升。然而,M2M 的当前标准缺乏全面的端到端的视图 M2M 生态系统。多个标准的机构

存在，缺乏细节，并没有解决终端到终端的观点。但是，标准往往是非常具体的和专注于一个特定的技术。例如，第三代合作伙伴关系项目安全体系结构 3 专注于具有用户标识模块的连接设备之间的接口的安全（例如，通用集成电路卡）和移动接入技术 。欧洲电信标准协会，作为 one M2M 成员，采取的是自上而下的方法定义服务创建设备。他们定义网络需求、访问技术和实际上是在其他标准组织或论坛范围内运行的设备。实际上在这些领域的影响仍然有待确定。一个全面的协议和不可知论者的标准将有助于使设备更易于开发和认证认识。

全球 M2M 连接，连接的移动设备在不同运营商和边界是具有挑战性的，需要一个集成的解决方案。这些挑战包括部署、配置、重新配置的 SIM 卡定位和远程管理。此外，自动化计费、报告、支持和运营管理流程与运营商不同，并向主机平台提供程序引入更复杂的要求。目前，（OTA）措施覆盖后端安全数据的生成和管理，提供最高安全级别，但这些平台是专为在网络内的本地服务而设计的。OTA 不会总是在漫游服务工作，可能不符合区域规定、性能标准和消费者的需求。为了实现物联网的全部效益和潜力，并点亮它的全球范围内的效应，需要有一个互操作的技术和适当政策讨论的国际论坛。

8. 结论及建议

存在一个较小的并且迅速的关闭窗口，以一种最大化安全性和最大限度地减少风险的方式控制物联网。如果国家不这样做，它将应对生成的后果。物联网的许多好处已经可以看到，包括效率的提升、故障的早期发现、可靠性和应变能力的提升。但是，新设备的快速和大量的连接带来了它的风险，包括新的攻击向量、新的漏洞，也许最让人关心的是，拥有用远程访问的能力从而造成物理破坏这个问题。

爆炸式增长以及与物联网的互联创造了一个 NS/EP 议题。数十亿的物联网设备（例如传感器、处理器和执行器），在一个封闭的网络中，有时通过更广泛的互联网，可以与其他每个设备进行通信，可以直接进入我们国家的关键基础设施系统。此外，许多个人和消费者的设备将连接到网络，这些网络有一些连接到关键系统，往往在不知情的情况下，为对手创造新的攻击途径。此外，以史为鉴，支持许多个人设备的技术将会集成到关键系统的设备中。

美国目前面临的网络安全问题，在某些方面，类似于掌控互联网协议发展的那个时代，那时候，安全并不是一个重要的考虑。在时间上，互联网的普遍使用的，从商业到全球通信甚至到生命维持，这种大规模范围是不可想象的。有早期的设计师的互联网设想了这一点，毫无疑问，他们会有更高的安全优先级。今

天,国家现在站在一个相似的改革边缘,这些改革包括如何与设备交互以及它们将如何为我们服务。但是,如果安全不作为一个核心被考虑,那么会有非常现实的后果,这些后果既有经济上也有生活上的安全。未来两到五年是获得这个权利的机会,在那之后,美国将会面临不作为的后果,并且冒着另一个错失的机会坚持在技术浪潮的早期安全方面。

根据新兴技术和动态威胁环境的迅速采用,立即采取行动是必要的,以解决动态物联网环境。NSTAC 发现:现有的治理、政策和制度的支持结构并没有被很好地配置,因此不能推动所需的快速变化;因此,NSTAC 建议前三个推荐在90 天内执行。由 EO13618 建立的基于权力与责任、国家安全和应急预备通信分配的功能,NSTAC 建议总统执行以下建议:

(1) 指导商务部,特别是 NIST 来开发物联网的定义,这些定义在各部门和机构在与物联网有关的评估中被使用。

(2) 指导管理和预算办公室,要求联邦部门和机构:

① 构建内部评估,以记录目前的物联网功能支持和/或计划支持的 NS/EP 的功能。这些评估必须考虑关联和相互依存关系,这些依存关系可能被引进,以及相关的风险和 NS/EP 利益方面。

② 开发应急计划以确定和管理所创建的由政府部署的目前和未来的物联网的安全问题。该计划应认识到物联网设备和他们的潜在用途将不断发展,此外,它不能完全担保预期的环境是绝对安全的,因为物联网的动态性质和存在潜在的威胁。

(3) 建一个物联网联合事务特遣队与现有组织机构协调促进安全、经济效益和潜在风险之间的平衡观点。至少,参加者应包括商务部、商务部国土安全部和国防部。专案组将设定里程碑完成下列活动,这些活动是要求解决风险紧迫性的反映,这些风险又是正在进行物联网部署对 NS/EP 产生的。

① 标示措施和新兴技术之间的差距,以解决独特的由物联网在 NS/EP 和制定计划的风险,如何激励发展的安全创新,以解决差距。

② 指导更新联邦战略文件,考虑物联网设备的爆炸性增长和依赖性方面的安全。例子包括确保网络空间安全,全面的国家网络安全倡议,以及可信的网络空间:战略计划联邦网络安全研究和开发计划等国家战略。

③ 指导更新现有的意识和培训计划。意识的焦点应该是告知公众,以及领导和决策者(私有和公共,包括议员),有关物联网的快速适应的利益和风险,因而,要鼓励周围的物联网设备的使用和开发安全。应考虑具体角色程序,因为这些涉及 NS/EP 系统的设计、开发、生产、采购和操作。

④ 鼓励和激励学术界开发课程的重点：ⓐ物联网，以及相关的安全挑战；及ⓑIT 和 OT 学科的收敛性，为了教育未来的从事设计的专业人士、管理人员或 NS/EP 系统的安全。

⑤ 鼓励参与到适当的国际标准和标准的国际论坛上，参与政策的发展。

（4）召集和促进政府和行业常设机构协调，协作和利用各种工业物联网联盟发展、更新和维护物联网部署准则来管理网络安全的牵连和风险。这些准则应包括物联网的集成度到系统中，这些系统是来支持 NS/EP 功能并突出市场可以解决的风险与国家安全风险之间的差距，这些风险是市场不打算解决的，它作为采购和操作程序的一部分被使用。结果应该启用自适应的指导方针，聚焦生态系统的网络安全和弹性，这种生态系统是以持续的合作过程为基础的风险及时变化的。执行机构必须有监督执行的权力和监督同意部署跨政府机构和部门的指导方针。

（5）指导 NS/EP 的沟通执行委员会开展以下工作：审查和推荐 NS/EP 更新计划，通过 PPD-1 更新过程优先推进下一代网络通信（例如，语音，视频，数据）和公共安全通信的发展；公布说明一些促进物联网增长、与 NS/EP 系统通信有关的数据；与私营部门协同更新 NS/EP 计划。

（6）指导科学和技术政策办公室审查当前的研发投资并建议未来的物联网安全的研发经费。这些研发经费将用于支持研究那些具有 NS/EP 功能的物联网系统所面临的潜在安全威胁和安全问题等相关课题。新技术的采纳和实施的度量提升，来自于国家的优先事项和利益联系，并确保已有的、类似的建议被适当地执行。随着建议的考虑和实施，对以下而言它将是重要的：①建立度量机制来度量和监督的推荐的有效性；②以最大限度地减少风险的方式纳入物联网技术；③将物联网纳入到目前的教育和意识计划中；④确保与物联网相关的研发项目正在解决不断变化的网络安全问题。NSTAC 认为这些举措将有助于最大限度地提高安全性以及物联网生态系统的弹性。

B.3　美国宽带互联网技术咨询组物联网安全和隐私建议报告简介

美国宽带互联网技术咨询组于 2016 年 11 月发布了一份《物联网安全和隐私建议报告》。该报告分析了为什么物联网安全和隐私问题非常重要，总结了目前物联网设备存在的诸多不安全因素，并给出了实现物联网安全和隐私保护的实践建议。

B.3.1 简介

在过去几年中，有很多的新设备连接到互联网中，它们不是个人计算机，而是有互联网连接功能的各种嵌入式设备。这种设备的示例包括恒温器、智能插头和网络摄像机。这类设备通常被称为物联网（IoT），显然，这种新型设备将在未来几年中有着强劲的增长，据不同角度的估计，预测到2020年将有数十亿此类设备[6]。

物联网设备的数量和种类正在快速增长；这些设备为终端用户提供了许多新的应用，并且在未来将提供更多功能。许多IoT解决方案已经可用或正在开发用于不久的将来部署，包括：

（1）传感器用于更好地了解人们的日常生活模式并监测健康；

（2）家庭监控和控制功能，从锁到供暖和供水系统；

（3）设备和应用软件，能够满足消费者需求并采取行动来解决他们的问题（例如监控库存并为消费者自动再订购产品设备）。

此外，当与数据分析和机器学习学科结合时，IoT设备可采取更主动的行动，暴露更有趣的数据模式，或向终端用户提出可改善他们的健康、环境、财务和其他方面的建议。

物联网的出现提供了一个从智能家居到智能城市的重大创新机会。不幸的是，许多IoT设备出现严重的安全和隐私缺陷[7]；B.3.2节分析了为什么IoT安全和隐私特别重要，B.3.3节详细讨论了许多最近的例子。这些缺陷使得终端用户以多种方式购买设备的风险，并且可能影响共享在相同网络链路上运行的其他用户的设备的互联网接入服务。这种缺陷还提供更广泛的缓解安全攻击问题的目标，互联网服务提供商（ISP）以及其他服务提供商（例如搜索引擎服务，基于Web的电子邮件和游戏站点），正引入重要的新的支持和缓解成本（通常传递给终端用户）[8]。这种缺陷还可以对设备制造商本身施加附加成本，来使设备制造商需采取措施来减轻这些问题。

更多情况下，IoT设备的开发、分发和维护过程需可以直接更改以防止遭受重大安全和隐私问题。BITAG认为，遵循本报告中概述的指南可以显著提高物联网设备的安全性和隐私性，并尽量减少影响对终端用户和ISP损害相关的成本。此外，除非物联网设备部门（制造和销售这些设备的行业部门）改善了设备的安全性和隐私性，否则可能会阻碍物联网消费市场的发展，并最终限制IoT对终端用户的承诺。

B.3.2　什么是物联网

物联网(IoT)包括传感器、制动器、控制器和活动记录器等设备。这些设备通常与网络上其他地方运行的软件交互,例如移动电话、通用计算设备(例如笔记本计算机)、公共互联网上的机器(例如"云")或这些组合等。物联网设备通常自主运行,无须人工干预。

术语"IoT"具有潜在的广泛范围。物联网可以是部署在家庭、企业、制造业、交通运输行业和其他行业的设备。因此,IoT 指的不仅仅是面向消费者的设备。

在本报告中,术语 IoT 仅指面向消费者的设备及其相关的本地和远程软件系统,尽管报告中的一些或所有建议可能应用更广泛,但本报告主要涉及消费者安装、配置和管理他们租用或拥有设备的情况。

1. 范围限制

该报告没有直接考虑用于工业、企业等的设备,如酒店或机场网络中的传感器、智慧城市、工业自动化、商业建筑控制或制造库存控制等。这些设置中,客户通常有资源和激励措施来指定和管理他们购买产品的安全和隐私功能。此外,它们中的很多设备不提供使用互联网可完全访问的商业无线连接。尽管如此,本报告中提到的一些问题也可能出现在这些环境中。

本报告的范围还限于发起或终止 IoT 设备的数据包。更具体地,本报告不关注那些发送或接受 IoT 设备以及其他业务(例如家庭网关、无线接入点或路由器)的设备的数据包。

此外,报告更关注那些使用 Internet 协议(IP)的设备和系统,无论是 IPv4 还是 IPv6 或两者。很多的物联网设备使用其他传输协议机制,如 Zigbee 1.0[9]、X10[10]等。这些设备需通过执行协议转换的设备才能连接到互联网。它们在隔离的网络上操作。然而,这里的建议仍然适用于执行协议转换的设备(例如家庭自动化中枢或网关)。

本报告重点介绍经 Internet 进行通信的本地 IP 网络上特定设备的问题。本报告的适用范围不包括未连接到公共 Internet 的隔离网络上发生的隐私和安全问题。

2. 用户已修改的 IoT 设备

一些设备可以运行用户自己安装的软件,而不运行制造商提供的软件。例

如,用户可以在设备上安装开源软件,而不是使用厂商提供的软件。所得产品可能受到本报告的考虑和建议的影响,但在这种情况下,设备应被视为用户负责的不同产品。

B.3.3 为什么 IoT 安全和隐私特别重要

物联网设备面临着与传统终端用户设备相同类型的安全和隐私问题。IoT 设备不会给用户提供明确的控制和文档来告知这些设备部署后会带来的风险。此外,研究表明,终端用户在安全和隐私决策上很容易出问题[11~13]。

(1) 消费者无相关技术且对其不感兴趣

终端用户缺乏评估特定物联网设备隐私和安全隐患的技术经验和兴趣[14]。此外,部署的 IoT 设备通常缺乏自动化机制来进行安全更新或执行安全策略[14,15]。

(2)发现和定位被攻击的设备存在困难

消费者难以识别和排除连接到他们家庭网络的设备所存在的故障[16]。当消费者将越来越多种类的物联网设备连接到他们的家庭网络时,这些设备将加剧这种情况。随时间的推移,用户很可能会忘记连接到他们网络中的设备,这将使识别和排除设备故障变得更困难。此外,ISP 难以帮助消费者识别安全问题的来源。虽然 ISP 能够确定客户家庭网络上的某个设备已遭到攻击,但由于 NAT 和其他隐藏的技术,使它们无法识别具体受损害的设备。

(3) 对互联网接入服务的影响

IoT 设备受到恶意软件攻击后,会发送或接收大量的数据包,从而影响 IoT 设备的用户和在同一共享网络链路上的用户的互联网访问服务。此外,这些设备也可能对用户和恶意软件攻击的其他用户造成威胁[17]。这恶意软件可用于发起 DDoS 攻击[18],发送垃圾邮件,攻击用户网络上的其他设备,或恶意干扰用户的互联网接入服务等。

这些问题增加了 ISP 的运营成本,使其必须花费大量经历来处理这些攻击,比如,为无法确定因特网服务异常的用户提供帮助和支持;当发现某些用户的设备正在执行恶意网络活动时,则断开他们的网络。这些问题还会降低互联网服务的性能并导致证书丢失,从而增加消费者的成本。最后,他们对攻击的目标和物联网设备制造商(或物联网供应链的其他部分)施加成本,因为制造商们需采取措施来减轻这些问题。

(4) 其他服务带来的影响

受恶意软件攻击的 IoT 设备可能会成为其他攻击的跳板,比如垃圾邮件和

拒绝服务攻击等，攻击者利用受损设备来发送和接收大量数据包[19]，从而干扰服务商提供的服务能力[20]。此外，受损的设备也可作为窃听本地网络信息或攻击其他设备及服务的“垫脚石”，进而产生数据泄露。对此，一些服务提供商，如搜索引擎、网络电子邮件和游戏网站等，必须投入精力来缓解这些攻击。同时，这些攻击的受害者也将承担财务和隐私的损失。此外，这些受损的 IoT 设备偶尔也会影响服务提供商的业务模型。例如，DNSChanger 恶意软件，就允许攻击者将他们自己的广告插入到受害者的网页[21]中。

B.3.4　许多设备不循序安全和隐私最佳原则

物联网设备已经成为滥用和攻击的跳板。很多研究人员发现现有物联网设备存在很多的安全隐私和风险[22~29]。未来几年，国家将部署数以万计的物联网设备，这将会成为发起攻击的大跳板——导致攻击者在用户家中的其他设备和互联网上偷偷收集终端用户或用户组的私人信息。除了消费者会遭受损失外，网络服务提供商遭受网络安全攻击事件的概率增加，导致网络运行成本上升。

最近的几个报告研究了物联网设备的安全和隐私特性，发现一些设备不遵守基本的安全和隐私最佳设计原则[30~36]。导致这种现象的原因包括：

（1）IoT 设备销售后缺乏开发、升级和部署的动力

对于零售商销售给消费者的 IoT 设备，设备供应商后期可能没有动力对软件进行更新。如果设备的收入仅来自初始销售，那么设备的任何维护都会受初始低利润的收入影响。这种支持供应商优先销售新设备而不维护现有设备的计划是不可行的。

（2）通过网络进行软件升级存在困难

IoT 设备的设计和配置使其不能通过网络进行软件更新，这会导致烦琐的更新过程。

（3）IoT 设备的资源有限

低利润销售的 IoT 设备，其硬件资源一般是有限的。所以，这些设备会缺乏某些基本安全措施，如加密、软件签名认证和安全访问控制等。此外，IoT 设备的计算和存储器受限，会导致设备主机上运行的安全软件或设备本身不能安全地进行升级。

（4）设备接口具有一定的约束

很多 IoT 设备的用户接口是受限的或不存在的。即便这些设备通过辅助装置来为用户提供接口时，这些接口的功能也可能很小。因此，这些 IoT 设备通常不能配置本地防火墙或禁用远程服务等。此外，这些 IoT 设备还可能缺乏向用

户显示错误信息和预警的能力。

（5）设备在制造过程中被植入了恶意软件

设备在制造或包装过程中，可能由生产人员或其他工作人员植入了恶意软件。这些被植入恶意软件的设备通常看起来工作正常，但它们却存在安全和隐私问题。此外，防火墙和网络隔离不能阻止这些设备攻击内部网络上的其他设备。

（6）设备制造商缺乏安全和隐私的经验

许多物联网设备制造商（以及物联网供应链的其他部分）在设计、开发、维护互联网连接设备或处理消费者数据上缺乏经验。例如缺乏安全开发的生命周期、事件响应团队，及安全和隐私工程经验等。

（7）存在安全隐患的设备带来的风险

以下示例说明了当 IoT 设备存在安全隐患时，可能会出现的问题及其程度。未经授权的用户此时能够：

① 执行未经授权的监控和监视

知道是否有特定的人在家，他们在哪个房间，以及他们什么时候进家；知道连接到家庭网络的其他设备，以及用户通过设备如何进行交互；远程激活设备上的麦克风或摄像头，来窃听或侦察一些人；通过发现门或车库最近是否被打开和关闭，来确定是否有人在家，进而帮助物理入侵；在物联网摄像机安装恶意软件，来访问摄像头获取的视频。

② 获得未经授权的访问或控制

在冬季关闭恒温器，导致水管爆裂，损坏家庭；打开或关闭灯，如关闭周边照明，来帮助物理入侵；打开门锁以帮助物理入侵；抑制来自门或窗传感器的报警；重新使用禁用的设备（例如比特币矿工）。

③ 导致设备或系统故障

激活住宅的空调系统来使电力网上产生意外的浪涌，从而试图产生掉电或停电；破坏健康数据收集传感器以修改健康数据，如血压、血糖或可被传输到健康监测服务或医疗装置（例如胰岛素泵）的重量信息；模拟设备管理软件，使其看起来正常运行，但却禁用了重要功能或更改了其他操作，导致设备或硬件系统在关键点上出现故障；防止恒温器控制建筑物的加热或冷却，导致极端的热或冷。

④ 干扰或骚扰用户

远程激活扬声器并进行口头威胁或骚扰；激活烟雾或其他安全警报。

所有这些情况都会为终端用户和整个互联网带来严重的安全和隐私风险。一些终端用户的安全和隐私风险也可能导致新形式的干扰。在一些极端情况

下，破坏收集的真实数据可导致人员伤害或死亡。对广泛部署的设备，其安全风险可以在数百或数千个设备上联合，进而在关键基础架构上制造分布式攻击。

物联网设备的安全和隐私问题可能会限制未来物联网行业的发展。一些严重的物联网安全事件可能会减少对物联网设备的需求，或限制物联网的潜力和增长。因此，解决安全和隐私问题，对支持物联网市场的长期健康、活力和增长是至关重要的。

B.3.5 IoT 安全和隐私问题观察

制造商不可能生产没有缺陷的软件；所有软件都有缺陷，生产没有缺陷的软件仍是一个未解决的难题。一些 IoT 设备出厂时所具有的软件是过时的，或随时间推移变得过时。软件带有缺陷不是问题，因为它是不能避免的；相反，我们应该担忧的是，制造商生产的设备中带有的过时软件，此软件包含许多重要的、已发现的安全漏洞，其中一些漏洞可能是设备首次连接到互联网发现的[37]。

其他 IoT 设备会安装一些带有已知漏洞的软件。即便这样，除非具有随时更新软件的机制，否则这些设备随时间推移，可能会发现漏洞，存在安全隐患。不幸的是，许多物联网设备缺乏稳定的自动化软件更新机制，该机制可在设备出厂和部署后及时修复漏洞。如果没有广泛采用稳定的自动化软件更新方法，未来几年，不安全和受损的物联网设备的数量会急剧增加。

随着时间的推移，存在安全和隐私问题的物联网设备，会成为一个可被黑客利用来执行攻击行为的新设备群体[38]。这些设备不仅对设备拥有者本身造成风险，而且还可能被利用或滥用于其他地方。因此，物联网设备的安全性不仅对制造商(以及物联网供应链的其他部分)和物联网用户，乃至整个互联网都是有意义的。

虽然本报告中列举了物联网设备中以前及现在存在的安全或隐私问题，但多数情况下，本文所举的例子可能在本报告发布之前已由相关单位解决。

1. 不安全网络通信

IoT 设备通常是资源受限的，缺乏传统计算设备(如移动电话、笔记本电脑和台式电脑等)的计算能力和带宽。因此，在物联网设备上很难实现通用计算设备中所应用的安全功能。例如，现在通信中常使用的 TLS 和 DTLS 都使用公钥加密体制在资源受限的 IoT 设备上是很难实现的。例如，Arduino 和 Raspberry Pi 物联网设备执行公钥加密或解密操作可能需要很多秒才能执行。

除了物联网设备及其运行的物联网平台存在限制外，该领域还发现了很多

安全缺陷，包括未加密的通信、物联网设备的数据泄露以及物联网设备连网所带来的不良影响。例如，某些 TLS 服务器实现容易受到“降级”攻击，由此攻击者可强迫服务器使用旧版本的 TLS 协议，这可能存在已知的安全问题，如中间人攻击。这种情况下，在 IoT 设备和支持云托管的服务之间进行通信可能会存在影响。

（1）未认证的通信

一些 IoT 设备提供没有认证和加密的自动软件更新机制，这种机制是不可用，且应该禁用的。更新机制和相关的命令及控制流应该被认证并加密，且设备与其他端点间通信的完整性应受到保护。遗憾的是，很多 IoT 设备在通信时不使用认证。例如，Lightwave RF 智能集线器每次重启时都会向远程服务器发送数据包，并每隔 15 分钟发送数据包来检查是否有软件更新。如果这样的通信是不安全，则能访问网络的攻击者很容易对其进行中间人攻击（man-in-the-middle attack）。

（2）未加密的通信

很多 IoT 设备以明文形式发送部分或所有数据，这意味着数据一旦“泄露”，很容易被其他设备或攻击者观察到。

结果一些 IoT 设备正泄露用户信息（例如向网络数据包的观察者），这可用于识别正在使用的 IoT 设备，并揭示当前用户活动和行为。例如：数码相框在同步照片时携带用户的电子邮件地址，并且当前的用户活动也清楚显示在其中；网络摄像机以明文方式发送视频文件；音频个人助理在明文中携带用户音频命令、传感器数据、用户电子邮件地址等；恒温器以明文方式携带当地气象数据和精确的用户位置信息，并可根据所使用的端口清楚地识别为特定品牌的恒温器；物联网设备集线器具有明确的一般和具体的数据包管理，这使得其可仅通过指纹来识别明文数据包，进而识别设备集线器；一些 IoT 支持的心脏起搏器的通信信道未加密。

以明文方式发送数据包不是当前部署所推荐的模式，因为它会在本地网络或互联网上泄露个人或其他信息。对于这一问题，互联网架构委员（IAB）最近表示：“IAB 督促协议设计者在默认情况下设计加密操作，强烈鼓励开发人员在其实现中使用加密，并对它们默认加密”。

（3）缺乏相互认证和授权

许多攻击源于网络边界，如家庭或其他地方的防火墙内。因此，防火墙内的通信不一定被认为是可靠的。因此，不论是在局域网还是互联网上的设备都需在设备之间建立信任；应该假设默认情况下其他设备是不值得信任的，故需明确

地认证和授权。设备允许未知的或未授权方更改其代码、配置或访问其数据，很可能导致设备受到威胁；设备可以显示其所有者的存在或不存在，执行恶意软件的安装或操作，或从根本上损害 IoT 核心功能。

幸运的是，与许多以联网通信为目的的笔记本电脑及通用计算设备相比，IoT 设备经常与少数特定的设备通信。例如，设备可能经常会与公开 DNS 名称和 IP 地址的控制或更新服务器通信，如果发现其与其他目标设备发生通信，则需引起关注。

（4）缺乏网络隔离

物联网设备不仅可在其所安装的家庭网络之外引入安全和隐私风险，还可能会产生新的风险，并且容易受到来自家庭内部网络的攻击。因为默认情况下许多家庭网络是不将网络的不同部分彼此分离的，所以网络连接设备可以观察或改变与同一家庭网络上的其他设备的数据包，因此一个设备观察或影响其他设备的行为。

尽管常用的做法是使用防火墙将网络上的设备彼此隔离，但是防火墙并不能防御设备或数据泄露，且它们不能防御已经安装在家庭网络内设备上的恶意软件。目前，典型的家庭网络在设备之间提供很少或没有隔离。

如果网络缺乏安全隔离，那某一个制造商或者有安全风险的设备会对网络上所有可被操作的设备的安全和隐私造成威胁。具体来说，攻击者可能会从同一网络上的其他设备收集个人信息。通常，家庭网络上的每个设备都可以看到来自同一网络上其他设备的数据包。如果设备以明文传输业务，则一个设备可能会发现另一设备的活动细节。最近的工作表明，即使只观察一些“粗略”的细节，如 DNS 查找及流量变化的能力，也可能会揭示关于设备活动和用户行为的信息。攻击者可通过控制设备推断出关于终端用户的重要信息，诸如可根据门传感器推断进入和离开家庭的时间，通过带有麦克风和摄像头的 IOT 设备获取音频和视频数据。许多家庭无线网络的安全设计成为攻击的跳板，攻击者可以利用这种平台攻击一个易受攻击的 IoT 设备，并利用该妥协作为从网络内部访问其他连接设备的机制。示例包括：

① 智能手表产品包括一个有效的 DNS 服务器，外部攻击者可以用来攻击智能手表连接到的网络上的其他设备。同一个产品有一个漏洞，允许本地网络数据包被外部网络攻击者查看。

② 智能灯泡可能被诱骗发送无线网络凭证，外部攻击者可以使用它来控制灯光和查看本地网络通信。

③ 一些设备制造商和 ISP 暴露了数百万设备和客户驻地设备（例如，调制

解调器、家庭路由器)的不安全远程管理接口,其全部共享相同的已知私钥,将这些设备暴露给被动和主动中间人攻击。

④ 某些型号的 VoIP 电话中的漏洞将允许本地网络攻击者向电话提供恶意固件升级。

⑤ Wi-Fi 安全摄像机的制造商设计他们的产品用对等网络软件,将“打”穿过本地网络防火墙的多个孔,不能轻易停用。该软件允许攻击者不仅科从各种各样的端点损害相机本身,而且还可对本地网络上的其他设备发起攻击。

2. 数据泄露

在家中安装 IoT 设备会增加数据泄露的潜力,因为这些设备可在云端或物联网设备之间泄露数据。

(1) 来自云端的泄露

目前,IoT 设备收集的大部分数据存储在家庭外的云服务中;这些云服务可能会因受外部攻击或内部威胁而遭受数据泄露。

此外,如果用户对这些云主机服务使用弱认证或弱加密,则用户数据也可能泄露。

几个例子包括:

① 与泰迪熊(在其鼻子上包含一个小型相机)相关联的 Web 应用程序包含一个安全漏洞,会导致儿童的身份暴露。

② 玩具娃娃使用一种易受降级攻击的 TLS 版本,在娃娃和云托管的服务器之间发送加密的聊天时,可以窃听儿童的录音。

③ 儿童工场的数据泄露暴露了 600 多万儿童的个人资料。

④ 机动车辆 Wi-Fi 接入点配置的缺陷导致车辆的位置被网站跟踪,从而获取 Wi-Fi 接入点名称及其位置。

⑤ 汽车制造商的系统向中央服务器以明文方式发送燃料经济性统计、精确的地理坐标、速度、方向和目的等信息。

许多数据泄露实例来自于已存在的设备。来自云端的数据泄露不是新的或特定的 IoT 设备,而云托管服务中的数据泄露的普遍对消费者 IoT 设备来说,是特殊问题,因为消费者 IoT 设备不仅日益普及,而且越来越多地收集个人和私人数据。

(2) 来自设备间的泄露

来自不同制造商的各种 IoT 设备可运行许多不同的应用软件,且可能都驻留在同一个局域网上。尽管标准 Wi-Fi 加密技术可保护局域网上数据传输的机

密性，但是仅使用加密不能保护用户隐私。

一些情况下，相同网络或相邻网络上的设备可观察来自其他设备的数据包。例如，设备可以将数据“泄露”给附近的设备或用户（在相同的局域网、Wi-Fi 网络上或简单地在附近）。即使使用了 Wi-Fi 加密技术，一个设备仍可观察到同一局域网上存在的其他设备，及以明文方式可见的一些设备的硬件地址（通常可以揭示设备的类型）。这种可见可使数字相框上的软件监视用户与相同网络上的其他设备的交互。

从一个设备泄露到另一设备的数据可包括家庭人员的姓名、家庭的精确地理位置，甚至消费者购买的产品的信息等。例如，最近的一项研究表明，家里的恒温器可泄露精确的地理信息。另一个最近的研究表明，研究人员的健身跟踪设备能通过蓝牙泄露加速度计数器数据，从而确定用户的 ATM PIN。

3. 易遭受恶意软件感染和其他滥用

用户设备上安装的恶意软件，通常会中断操作，获取未授权的访问或发起攻击，也可通过各种机制感染 IoT 设备。同时，还可发生其他形式的滥用。一些示例包括：

① 制造商可能无法充分保护软件供应链，从而允许恶意软件被放置在物联网设备的最初软件上。

② 设备可附带包含已知漏洞的过期软件。当用户将设备连接到网络时，设备立即成为攻击者的目标。过去的研究表明，“生存时间”（即，设备在感染之前连接到网络的时间）在一些情况下可少于 10 分钟。如果带有过时软件的设备在出厂时，不立即检查软件更新，则它存在立即被感染的风险。

③ 软件更新机制可能不包括软件加载的认证，该认证用以确保软件的来源是可信的。通过社交工程，用户可能受到影响或被诱导而将受损软件加载到 IoT 设备上。

④ 软件可包括利用（具有或不具有用户参与）命令行能力或应用编程接口（API）来将恶意软件加载到 IoT 设备上。

⑤ 设备开放不必要的端口是不安全的，如 telnet。这些不必要的端口可被用于危害设备，例如指示设备访问目的地以下载恶意软件。不必要的端口也可以用于放大攻击。

⑥ 设备使用默认弱认证，例如常见的或易于猜到的用户名和密码（例如，“admin”，“password”）。此外，远程访问的认证可能不受保护，使得实际上不在家中的其他人登录到设备并在其上安装恶意软件。

4. 服务中断的潜在因素

设备存在或受到攻击时，服务的可用性是物联网设备安全性的一个重要方面。可用性或连接性的潜在损失包括能降低 IoT 设备的功能，以及在一些情况下会降低设备的安全性，例如 IoT 设备没有连接时，将不能工作（例如，连接是丢失）。IoT 设备可遭受多种方式的服务中断。

云托管应用程序失去支持。如果设备依赖与云服务的通信，那么当设备与云服务失去连接时，该设备可能无法工作。这种中断可能是各种原因导致的，包括互联网连接中断，云软件服务中的缺陷，供应商或制造商停业，或消费者停止服务订阅等。

失去与网络的连接。家庭网络内的连接可被中断，例如可由未插入的电力电缆、对 Wi-Fi 的无线电干扰或决定限制访问防火墙等导致中断。

设备损坏。设备可能物理损坏，或其软件可能损坏或以其他方式无法操作（有时称为“刺穿”设备）。

“物理或逻辑损坏”的设备可能是不可恢复的，它依赖于与云托管服务通信的设备在通信恢复时可能再次可操作。

中断某些服务可能会损坏财产，并使用户处于危险之中。例如，物联网恒温器中的软件缺陷导致无法操作家庭供暖系统，从而使家庭中的管道冻结。加热和冷却系统的故障可能导致死亡。当物联网设备负责从个人健康到家庭安全的一切时，用户安全的风险很高。

5. 设备安全和隐私问题持续存在的潜在因素

许多 IoT 设备可能永远不会接收软件更新，一方面是因为制造商（或物联网供应链中的其他方或 IoT 服务提供商）可能不提供更新，一方面是因为消费者可能不应用已经可用的更新。相似类型的设备有许多例子。

（1）许多物联网设备将永远不会被修复

安全漏洞的关键软件的部署、更新、修补通常很困难，这对物联网设备构成了独特的挑战。原因如下：首先，许多设备供应商和制造商没有将软件更新部署到数千个设备（或更多）的系统或过程中。其次，通过网络部署更新在消费者家庭中操作的设备是困难的，因为更新时可能中断服务，一旦不正确地执行，则有可能“毁坏”设备。此外，一些设备甚至不能进行软件更新。

消费电子行业出现了三种软件更新方法，其中两种依靠用户采取行动（一个根本缺陷），而第三种是自动的，无须用户操作。在实践中，每种方法的效用各不

相同。这些方法如下：

① 用户启动的软件更新。此方法要求设备的本地管理员手动启动对设备的任何软件更新的检查和安装。这种方式的一个典型例子是市场上的在零售家庭网关或路由器设备。他们中的一些设备需要用户从制造商的网站下载新的软件镜像，然后访问本地设备管理网页，找到用于软件升级的接口并上传文件。这个过程不仅耗时，而且对让设备以“足够好”的方式工作的非技术人员或临时用户而言可能是非常可怕的。

② 用户批准时自动检查更新软件。这些设备会定期检查新的软件更新。当更新可用时，设备向用户呈现是否允许继续更新的询问提示。智能电视和控制台游戏设备经常使用这种方法。在这些情况下，应用任何特定的软件更新可能需要几分钟或更长时间，这是为什么向用户呈现推迟安装的选项的原因。

③ 全自动软件更新。有些设备会定期检查新软件是否可用；如果是，他们将下载软件并安装，无须用户干预。在一些情况下，设备可以在一天的特定时间，例如深夜或存在一段时间内没有与设备有关的活动时执行更新，以使用户的中断达到最小。不幸的是，自动化软件更新也存在一些挑战，如对存在数据上限（如果适用）的用户来说，更新软件时很可能引入新的缺陷。

软件更新的常见方法是用户发起或用户批准，这两种方法都会导致相对较低的更新率。因此，拥有和维护（COAM）数百万消费者的家庭网关很可能永远不会接受软件更新。例如，NetGear 型号的一些家庭网关附带一个软件缺陷，导致这些设备对 ISP DNS 服务器执行洪泛攻击，以每秒成千上万的 DNS 请求，每天请求数增加多达数百万，或大量的 NTP 到 NTP 服务器查询。虽然这个特定的软件缺陷已经报道了许多年，但网络运营商仍然发现这些设备在运行对网络有不良影响的较旧的软件，因为这些软件的缺陷而无意中会执行 DDoS 攻击。

（2）软件更新解决的不仅仅是缺陷

同样值得牢记的是，软件更新不仅仅用于修复安全或隐私的缺陷。它们还可以用于引入核心新功能。而且这些新功能一般与性能和安全性相关，例如与 IPv6 寻址、DNS 安全扩展（DNSSEC）验证和 TCP 缓冲器控制（例如，“缓冲膨胀”）或活动队列管理（例如，AQM）。

（3）消费者不太可能更新物联网设备软件

少数终端用户会一贯地更新符合他们的设备软件，除非他们被设备的图形用户界面（GUI）不断强制地提醒这样做（例如，PC 上的常规弹出窗口，移动应用商店中的计数器，弹跳应用程序图标等），这在人机交互学科中能很好地理解。其他近期的工作表明，用户因各种原因放弃在固定和移动设备上执行软件更新，

其原因包括工作周期的中断和与软件更新相关的数据成本。

尽管用户不对软件进行更新能保障对 IoT 设备进行深入研究，但是这种情况可能比常规或非 IoT 设备更糟糕。除了用户对于软件更新存在风险的行为，许多 IoT 设备缺乏 GUI 或其他指示器，来表明新软件可用或必要。此外，设备的数量与种类的增加使得跟踪软件更新对典型的互联网消费者是难以完成的任务。因此，对于物联网设备，最好假设大多数终端用户不会自己采取行动来更新设备上的软件。

6. 设备更换可能是软件更新的替代方法

一些情况下，完全替换设备可能是软件更新的替代方法。一些 IoT 设备可如此便宜，以至于更新软件可能是不切实际或不具成本效益的。例如，成本为 0.99 元的充电适配器可能具有一些受限的 IoT 功能。以该设备的单位成本来说，更新设备可能不经济；相反，可能更有意义的是回收设备并用新设备来替换。然而，这种方法需要以下元素来提供软件更新的安全替代：一种方法来识别设备中一个或多个累积的漏洞何时损害设备，及它应该被替换的时间点；一种方法是在设备被确定为易受攻击时禁用与设备的通信。潜在方法的示例包括从网络远程禁用设备或阻止从家庭网关对设备的访问；一种方法是通知用户设备间的通信已经禁用。

即使在这些情况下，用户仍可能不愿停止使用设备，只要它部分地继续起作用。一旦设备的通信能力禁用，则继续使用不应存在安全漏洞。

B.3.6 家庭网络技术的可能作用

设备制造商对他们的设备使用默认保护构成了提高物联网安全性和隐私的重要步骤，但这还是远远不够的。即使未被恶意软件感染的 IoT 设备仍可能窃听其他家庭网络数据包（例如，通过制造商或第三方安装软件），从而危及用户隐私。家庭通常被认为是存在防火墙或隔离的环境，并且多个不相关的 IoT 设备通常在该防火墙内具有不受限制的访问。此外，家庭网络中的单个不安全或受损设备可能成为攻击的跳板，所以“深度防御”至关重要。

最近的研究和报告表明，不久的将来，家庭网络设备可能需要有一些角色来控制和管理物联网设备之间以及与互联网之间通信的数据包。这种网络设备的能力包括：

（1）自动发现家庭网络连接的设备及其清单。

（2）向用户呈现有以下信息：①设备正在向互联网的哪些部分发送什么数

据；以及②设备正在与家中的什么设备进行通信，如过去智能手机和浏览器所做的。

（3）向用户提供简单方法以防止或禁止单个设备与家庭网络上的其他 IoT 设备通信或与云中的存储服务器通信但不损害设备的主要功能。最近的一项研究使用两个物联网设备示例，一个是飞利浦 Hue 灯泡，另一个是 Nest 恒温器。

提高网络安全性和隐私性的技术最终只采取多种形式中的一种。与 ISP 提供的设备分离（例如，IoT 集线器或单独的家庭路由器）或与 ISP 提供的设备集成的家庭网关可以在网络内执行测量，以帮助用户理解家庭中的 IoT 设备以及这些设备之间的复杂数据流乃至家庭外的第三方网站和服务。某种意义上说，监视家庭中的设备数据包可能最终有助于提高这些 IoT 设备行为的透明度。

通过集线器监视和管理 IoT 数据包和来自端到端的安全性之间存在的一些冲突数据包。值得注意的是，即使发送和接收这些设备的网络数据包是端到端加密的，某些特征（例如任何特定设备正在与之通信的其他设备和位置）仍可从该流量中明显看出。标准化以允许使用这种 IoT 集线器的协作式业务分类和保护将允许设备是生态系统的被识别和认证的部分，使得管理具有在选择加入的基础上对业务发起者可用的细粒度控制。

除了简单地帮助可视化这些业务流外，这样的网关可以实施合理的默认设置以改进连接的 IoT 设备的安全性和隐私。例如，最近的研究表明，家庭网络防火墙可以防止某些设备将日志和其他信息泄露给第三方云提供商，且不会削弱设备本身的功能。识别可以安装在网关处的合理的默认防火墙设置，来改善安全性和隐私是一个开放的问题。假定这样的家庭网络防火墙可能引起“隐私军备竞赛”（例如，可以想象设备制造商不向阻止设备的跟踪能力的用户提供安全更新），则制造商与供应商的设备认证一方面可以确保消费者保持对这些设备彼此之间及与第三方站点和服务进行通信的知悉选择。

最后，物联网设备之间的交互可能需要更复杂的中介。例如，虽然用户通常不希望某些设备彼此通信或交互，但特定情况下，是可存在允许用于特定任务的设备之间的通信或交互的。作为一个可能的示例，应考虑一些用户可能想在家中观看电影时自动地使灯变暗等情况。在这种情况下，应用可能涉及流设备（例如，Roku 或 Apple TV）与智能插头和开关（例如，Belkin WeMo 开关）之间的媒介通信。另一方面，一般来说，用户可能不希望这些设备的交互，甚至观察彼此的业务。因此，与适当用户接口耦合的网关可最终为这种类型的复杂介导的交互提供更好的机会。

最近的报告表明，许多这些目标很可能达到。例如，研究人员使用家庭网络防火墙来防止 Nest 恒温器将其状态日志发送到云，而不会损害设备本身。然而，由于典型用户不太可能配置防火墙规则，所以这些防火墙功能必须更可用，并且如果可能的话，在被认为可行之前必须是自动的。

B.3.7 建议

报告的这一部分表达了 BITAG 技术工作组(TWG)的建议。尽管本报告前面的部分已经讨论了长期前瞻性解决方案的潜力(例如，家庭网络技术在减轻设备不安全方面的作用)，本节重点介绍 BITAG 认为可以使用现有技术在短期内采取行动的建议。

1. IoT 设备应使用最好的最新软件实践

(1) 物联网设备应提供合理的最新软件

BITAG 建议物联网设备应提供给客户或零售网点最合理的最新软件，这些软件不包含严重、已知的漏洞。然而，由于软件缺陷是“生活的事实”，并且当设备在货架上时发现新的漏洞并不罕见。所以物联网设备具有自动安全的软件更新(见下一个项)机制是至关重要。

(2) IoT 设备应该具有自动安全软件更新的机制

应该尽量减少软件的缺陷，但是，如上所述，它们是不可避免的。因此，物联网设备必须具有自动安全的软件更新机制。

BITAG 建议物联网设备制造商或物联网服务提供商在设计其设备和系统时，应假设可随时发现新的错误和漏洞。他们应该设计系统和流程来确保物联网设备软件的自动更新，而不需依赖任何类型的用户操作，甚至用户选择。

(3) IoT 设备应默认使用强认证

BITAG 建议默认情况下保护 IoT 设备(例如密码保护)，不使用常见或容易猜到的用户名和密码(例如“admin”“password”)。同时应保护用于远程访问的认证，因为其可能允许物理上不在家中的其他人监视或控制家庭内的情况(例如，改变气候控制，监视用户活动)。每个设备的身份认证凭据必须是唯一的。

满足这些标准的默认认证方法包括：每个设备使用固定的默认密码，但要求用户在安装过程中(即在设备运行之前)改变它；每个设备的每个单元使用唯一密码，并将对应的密码附加到设备的标签上。

(4) IoT 设备配置应进行测试和加固

一些 IoT 设备允许用户定制设备的行为。BITAG 建议制造商测试每个设

备的安全性和一系列可能的配置,而不是简单地使用默认配置。设备的接口应主动阻止用户使用不太安全的方式配置设备。

2. IoT 设备应遵循安全和加密的最佳实践

BITAG 建议物联网设备制造商使用基于传输层安全(TLS)或轻量级加密(LWC)保护的通信。一些设备可以实时地执行对称加密。此外,提供轻量级加密(LWC)的额外选项,用于保护资源受限设备的通信数据包。如果设备依赖于公钥基础设施(PKI),则授权实体必须能够在受到攻击时及时撤销证书,如 Web 浏览器和 PC 操作系统所做的。云服务可以通过证书透明度来加强颁发的证书完整性。最后,制造商应注意避免使用弱的加密方法、协议和密钥大小。

依赖云托管的供应商应鼓励物联网设备按照最佳实践原则配置他们的服务器,如将 TLS 实施配置为仅接受最新 TLS 版本。

(1) 默认通信加密配置(命令和控制)

使用未认证或明文通信来管理设备会带来重大的安全风险。BITAG 建议用于设备管理的所有通信都需在经过认证且安全的通道上进行。

(2) 来自 IoT 控制器的安全通信

如果物联网设备使用集中式控制器来与网络中的云服务通信,则 BITAG 建议要在两个方向上确保通信信道的安全。

(3) 加密本地存储的敏感数据

BITAG 建议任何敏感或机密数据(例如,私钥、预共享密钥、用户或设施信息)需加密存储。

(4) 通信、软件更改和数据请求的认证

BITAG 建议 IoT 设备需对与其通信的端点进行身份认证。认证需要验证端点的身份,这又涉及认证端点正在使用的证书应是由设备信任并且尚未撤销的证书颁发机构签名的。

(5) 每个设备使用唯一证书

BITAG 建议每个设备具有唯一的证书。如果设备使用公钥加密技术(例如,签署消息、交换会话密钥或认证自身),则每个设备应当具有唯一的可验证证书。如果设备使用对称密钥加密,端点不应与其他方共享对称密钥。

(6) 使用可以更新的证书

BITAG 建议设备制造商应支持一种安全机制,通过该机制可以更新设备使用的证书。然而,安全地实施该推荐需要特别注意,因为不正确的实现本身可能引入新的攻击力量。

（7）关闭不必要的端口并禁用不必要的服务

BITAG 建议设备制造商关闭不必要的端口，例如 telnet，因为不必要的端口可能是不安全的，否则可能被损坏。设备应关闭或禁用不使用的管理接口和功能。设备也不应提供设备未使用的驱动程序。

（8）使用积极维护和支持的库

本报告中的很多建议需要通过安全的通信渠道执行。然而，本地实现的加密协议和安全信道本身可能会引入漏洞。BITAG 建议，在实施本报告中的建议时，设备制造商应尽可能使用积极支持和维护的库和框架。

3. IoT 设备在通信中应是受限而不是允许的

BITAG 建议物联网设备仅与可信端点通信。如果可能，默认情况下不应通过入站连接访问设备。IoT 设备不应该仅依靠网络防火墙来限制通信，因为家庭内的设备之间的一些通信可能不需穿过防火墙。

注意，BITAG 建议限制物联网设备通信的配置不应以开放生态系统为代价。用户应该能够配置任意 IoT 设备之间的通信，并且应该允许彼此受信的设备进行通信。安全通信可引导反映任何给定设备期望和与之通信设备集合的受限信任列表。这些设备间通信应允许在有可信机制且安全的信道上进行。

4. IoT 设备在网络连接中断时应继续工作

BITAG 建议物联网设备在未联网时，仍应能够执行其主要功能（例如，灯开关或恒温器应继续与手动控制一起工作）。这是因为互联网连接可能因偶然的误配置或受恶意攻击（例如，拒绝服务攻击）而中断；设备在面对这些类型的连接中断时应在功能上是鲁棒的。

对用户安全有影响的 IoT 设备应在断开连接的操作下继续工作，以保护消费者的安全。在这些情况下，设备或后端系统应通知用户故障。

在可能的情况下，设备制造商应该让用户很容易地禁用或阻止（例如，使用防火墙）各种网络的数据包，且不会妨碍设备的主要功能。

5. 设备在云端失败时应继续工作

在云后台的连接中断或云服务发生故障时，那些依赖或使用云后台运行的服务应该继续提供，即便是使处于降级或部分功能状态。例如，可通过云服务来改变恒温器的设置，使其在最坏的情况下仍能继续使用默认已知的设置来运行。即便在网络连接失败时，也应该可以从家里访问云托管的家庭安全摄像机。

6. IoT 设备应支持寻址和命名的最佳实践

许多物联网设备在安装之后可能仍需部署多年。因此，物联网设备应支持用于 IP 寻址和使用域名服务系统(DNS)的相对最近的、最新的最佳实践。支持用于寻址和命名的最新协议将确保这些设备在未来几年内保持正常运行，性能良好，并且能够支持基于 DNS 的重要安全功能。

(1) IPv6

BITAG 建议物联网设备支持最新版本的互联网协议 IPv6。

(2) DNSSEC

BITAG 建议，当使用域名时，IoT 设备应支持验证或使用 DNS 安全扩展功能(DNSSEC)。例如，如果 IoT 设备使用 example. com 域与云服务进行通信，则云提供商应该能够对此域名进行签名，IoT 设备应能够验证该签名(或确保其上游 DNS 解析器已经这样做，并在 DNS 响应中指出这一点)。

7. IOT 设备应提供易于查找和理解的隐私政策

BITAG 建议物联网设备附带隐私政策，但该隐私政策对于典型用户必须易于查找和理解。

8. 揭示远程降低 IoT 设备功能的权限

BITAG 建议，如果 IoT 设备的功能可以由第三方(例如制造商或 IoT 服务提供商)远程降低，则应在购买时向用户明确说明这种可能性。

9. IoT 设备行业应考虑网络安全行业计划

BITAG 建议物联网设备行业或相关的消费电子集团应考虑创建一个行业支持的程序，这种程序可以在物联网零售包装上携带某种“安全物联网设备”的标志或符号。这样的程序可以类似于 Wi-Fi 联盟或其他符合各种标准和(或)最佳实践的方式的验证设备。

业界支持的一套最佳实践似乎是在物联网创新与网络安全流动性相关的安全挑战之间取得平衡的最务实的手段，它避免了认证过程中可能出现的核对表态。

10. IoT 供应链应在解决 IoT 安全和隐私问题中发挥作用

在今天的工厂到零售供应链中，随时间推移，通常很难定义每个参与方所发

挥的作用。故在此简称为“物联网供应链”。物联网设备和其他终端设备的用户依赖物联网供应链来保护他们的安全和隐私,物联网供应链的一些或所有部分在产品的整个生命周期中发挥着关键作用。除了本章中的其他建议,BITAG 建议物联网供应链应采取以下步骤:

(1) 设备应具有清晰易懂的隐私政策,特别是在设备与正在进行的服务一起销售的情况下。

(2) 设备应该具有物联网设备的重置机制,当消费者返回或转售设备时,清除所有配置以供使用。设备制造商还应该提供一种机制来删除或重置相应设备在云中存储的任何数据。

(3) 制造商应提供错误报告系统,来明确定义缺陷提交机制和响应策略。

(4) 制造商应构建安全的软件供应链,以防止在制造过程中引入恶意软件;供应商和制造商应采取适当措施,确保其软件供应链安全。

(5) 制造商应支持物联网设备在整个过程中其生命周期安全可靠,从设计到设备退役的时间,包括计划为其提供持续支持的时间段的透明度,以及消费者应该从设备的寿命结束时的功能。

(6) 制造商应为消费者提供明确的方法,以确定他们可以得到那些支持,以及联系消费者以告知有关软件漏洞或其他问题的信息的人。

(7) 制造商应报告发现和修复软件漏洞,这些漏洞构成对消费者安全或隐私的威胁。

(8) 制造商应提供一个脆弱性报告流程,其中包含一个定义明确、易于定位和安全的漏洞报告清单,以及一个记录的响应策略。制造商应考虑遵守一个处理漏洞报告的标准,如 ISO 30111。

B.3.8 其他小组

虽然 BITAG 在这个问题上有一个独特的见解,值得注意的是几个其他组织也有研究集中在物联网安全和隐私工作的各个方面。这些团体包括:

- 智能对象联盟协议(IPSO)
- 电气和电子工程师协会(IEEE)
- 国家标准与技术研究所(NIST)
- 互联网工程任务组
- LWIG(轻型实施指南)
- 6Lo(资源约束节点的网络上的 IPv6)
  - 6TiSCH(IEEE 802.15.4e 的 TSCH 模式上的 IPv6)

  * ROLL(在低功率和有损网络上路由)
  * CoRE(约束 RESTful 环境)
  * DICE(约束环境中的 DTLS)
  * ACE(约束环境的认证和授权)
  * COSE(CBOR 对象签名和加密)
  * 6lowpan IPv6 over 低功率 WPAN(关闭)
- GSMA:互联生活
- IRTF:互联网研究工作组
  * T2TRG:Thing-to-Thing 研究小组
- W3C:全球 Web 联盟
  * WoT:网络兴趣组
- 美国联邦贸易委员会(FTC)
- 美国商务部,国家电信和信息 给药(NTIA)
- 互联网治理论坛(IGF)
- 在线信任联盟
- 国际标准化组织联合技术委员会 1(ISO/IEC JTC1):成立了两个关于管理和物联网的特别工作组;一个由 ANSI 管理。
  * 国际电工委员会:虽然 IEC 不仅限于物联网设备(并且工作在所有电气/电子技术),它已经做了几个可能有标准的研究论文。
- 国际信息技术标准委员会(INCITS):由 ANSI 认可,"作为全球努力的中央美国技术咨询小组"。
- TRUSTe 多方利益相关者物联网隐私技术工作组:旨在制定技术标准,帮助公司开发解决方案,保护 IoT 中的消费者隐私。
- 电气和电子工程师协会(IEEE)P2413:关于物联网建筑框架标准的 IEEE 项目。
- 无线 IoT 论坛:"不是一个标准组织,而是旨在向缺乏标准(例如长距离无线连接)的标准机构提供要求,并在存在竞争标准(如家庭设备发现)"。
  * 应用程序组:审核标准 API 的工作组
  * 连接组:评估无线电接入的工作组
  * 监管小组:协调全球许可证豁免条例和许可频谱可用性的工作组
- 开放互连基础(以前称为开放互连联盟):由英特尔、思科和三星创建的组织,为 IoT 创建开放的互操作规范。也获得 UPnP 论坛。

- 对象管理组(OMG):一个国际非营利技术标准联盟,负责工业物联网的主要工作。
  * 工业互联网联盟:"……是开放的成员,国际非营利性联盟……设置工业互联网的架构框架和方向。"致力于加速采用专用于物联网市场的无线广域网技术。由思科成立,包括埃森哲、阿尔凯萨、BT 泰伦萨和 WSN。
- one M2M:开发技术规范,满足对可以嵌入各种硬件和软件的通用 M2M 服务层的需要
- 国际自动化协会(ISA):"非营利专业协会,为那些应用工程和技术改善现代自动化和控制系统的管理,安全和网络安全的人制定标准"。对物联网做了一些研究,虽然没有工作组的说明。
- OASIS:"非营利性联盟,推动全球信息社会的开放标准的开发,融合和采用"。
  * OASIS 高级消息队列协议(AMQP)TC:定义用于处理业务消息传递的无处不在、安全、可靠和开放的互联网协议。
  * OASIS 消息队列遥测传输(MQTT)TC:提供适合于在 M2M/IoT 上下文中的通信的轻量级发布/订阅可靠消息传输协议,其中需要小的代码覆盖区和/或网络带宽是溢价的。
  * OASIS 开放式建筑信息交换(oBIX)TC:使建筑中的机械和电气控制系统与企业应用程序进行通信。
- Hypercat:一个为工业和城市推动安全和可互操作的物联网的联盟和标准。
- AllSeen 联盟:创建 AllJoyn,这是一个"协作,开放的生态系统"。
- 线程组:创建 Thread 协议,这是一个免版税的物联网网络协议。提供产品认证。

小结

本附录以物联网安全的视角,介绍了美国近年来在物联网安全(尤其是工业物联网安全)领域所制定的安全战略和建议报告,介绍了物联网安全战略安全保障原则,物联网设备与系统安全防护注意事项,及物联网安全和隐私保护建议等。

参考文献

[1] DHS. Strategic Principles for Securing the Internet of Things. https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[2] NIST. Framework for improving critical infrastructure cybersecurity. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[3] ICS-CERT. Recommended practices. https://ics-cert.us-cert.gov/Recommended-Practices

[4] NSTAC. NSTAC report to the President on the Internet of Things. 2014. https://www.dhs.gov/sites/default/files/publications/IoT%20Final%20Draft%20Report%2001—2014.pdf

[5] BITAG. Internet of Things(IoT) security and privacy recommendations. https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

[6] Mckinsey & Company. James Manika et al. The Internet of Things: mapping the value beyond the Hype. http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx

[7] Krebson Security, Blog. IoT reality: smart devices, dumb defaults. http://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/

[8] Kalev Leetaru. How the internet of Things will turn your living room into the future cyber battleground. https://www.forbes.com/sites/kalevleetaru/2015/11/06/how-the-internet-of-things-will-turn-your-living-room-into-the-future-cyber-battleground/#4197241b65c9

[9] IEEE Standards Association. IEEE 802.15: Wireless Personal Area Networks(PANs). https://standards.ieee.org/about/get/802/802.15.html (last visitedNov. 18, 2016)

[10] X10. https://www.x10.com/(last visitedNov. 18, 2016)

[11] Hewlett Packard. Internet of Things research study: 2015 report. https://www.hpe.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf

[12] John Pescatore. Securing the Internet of Things Survey, Sans Institute Analyst Survey, Jan. 2014, https://www.sans.org/reading-room/whitepapers/analyst/securing-internet-things-survey-34785

[13] ZDNet. Charlie Osborne. Internet of Things devices lack fundamental security, study finds. http://www.zdnet.com/article/internet-of-things-devices-lack-fundamental-security-study-finds/

[14] Ka-PingYee. Aligning security and usability. http://zesty.ca/pubs/yee-sid-ieeesp2004.pdf

[15] Veracode. The Internet of Things: security research study. https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf

[16] RebeccaE. Grinter, et al. The work to make a homenetwork. http://www.cc.gatech.edu/~beki/c27.pdf

[17] Yin Min Pa Pa, et al. IoT POT: analysing the rise of IoT compromises. https://www.usenix.org/system/files/conference/woot15/woot15-paper-pa.pdf

[18] Symantec. IoT devices being increasingly used for DDoS attacks. http://www.symantec.com/connect/blogs/iotdevices-being-increasingly-used-ddos-attacks

[19] Steve Rogerson. IoT blamedfor denial of service attacks. http://www.iotm2mcouncil.org/serviceattacks

[20] Energin Janina. Distributed denial-of-service (DDoS) attack knocked the file-sharing site pirate bay offline. http://ceoworld.biz/ceo/2012/05/17/distributed-denial-of-service-ddos-attack-knocked-the-file-sharing-site-pirate-bayoffline

[21] Angela Moscaritolo. FBI arrests six in click-fraudcyber scam that netted $14M. http://www.scmagazine.com/fbi-arrests-six-in-click-fraud-cyber-scam-that-netted-14m/article/216399/

[22] Sarthak Grover, Nick Feamster. The Internet of unpatched things. https://www.ftc.gov/system/files/documents/public_comments/2015/10/00071-98118.pdf

[23] Bruce Schneier. The Internet of Things is wildly insecure-and often unpatchable. https://www.schneier.com/essays/archives/2014/01/the_internet_ of_thin.html

[24] Bruce Schneier. Surveillance and the Internet of Things. https://www.schneier.com/blog/archives/2013/05/the_eyes_and_ea.html

[25] Matt Loeb. Internet of Things security issues requirea rethink on risk management. http://blogs.wsj.com/cio/2015/10/14/internet-of-things-security-issues-require-a-rethink-on-risk-management/

[26] Arik Hesseldahl. A hacker's-eye view of the Internet of Things. http://recode.net/2015/04/07/ahackers-eye-view-of-the-internet-of-things/

[27] Arik Hesseldahl. The Internet of Things is the hackers' new playground. http://recode.net/2014/07/29/the-internet-of-things-is-the-hackers-new-playground/

[28] Julie Knudson. Security challenges of the Internet of Things. http://www.enterprisenetworkingplanet.com/netsecur/security-challenges-of-the-internet-of-things.html

[29] Reddit. "I bought and returned a set of WiFi connected home security cameras, forgot todelete my account and can now watch the new owner" https://www.reddit.com/r/privacy/comments/4ortwb/i_bought_and_returned_a_set_of_wifi_connected/

[30] Christina Cardoza. Princeton tires to find out if your IoT devices are safe. http://sdtimes.com/princeton-tries-to-find-out-are-your-iot-devices-safe/

[31] Christian Dancke Tuen. Security in Internet of Things Systems. http://metalab.uniten.edu.my/~azie/AllArt/13009%20-%202015%20-%20Christian%20Dancke%20Tuen%20-%20Security%20in%20Internet%20of%20Things%20Systems%20(MASTER%20Thesis).pdf

[32]　Hewlett Packard. Internet of Things security study: smart watches. http://go. saas. hpe. com/l/28912/2015-07-20/325lbm/28912/69038/IoT_Research_ Series_ Smart watches. pdf
[33]　Kim Zetter. Hospital networks are leaking data, leaving critical devices vulnerable. https://www. wired. com/2014/06/hospital-networks-leaking-data/
[34]　Mario Ballano Barcena, Candid Wueest. Insecurity in the Internet of Things. https://www. symantec. com/content/en/us/enterprise/fact_sheets/b-in security-in-the-internet-of-things-ds. pdf
[35]　Katie Natopoulos. Somebody's watching: how a simple exploit lets strangers tap into private security cameras. https://www. theverge. com/search? q=Somebody%E2%80%99s+watching%3A+how+a+%09simple+exploit%09+lets%09+stranger+s%09tap+into+private+security+cameras
[36]　Brian Krebs. This is why people fear the Internet of Things. https://krebsonsecurity. com/2016/02/this-is-why-people-fear-the-internet-of-things/
[37]　Swati Khandelwal. IoT Botnet-25,000 CCTV cameras hacked to launch DDoS attack. http://thehackernews. com/2016/06/cctv-camera-hacking. html
[38]　BITAG. SNMP Reflected amplification DDoS attack mitigation. https://www. bitag. org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation. pdf